TURVALLISUUSKONSEPTIN TOTEUTUKSEN AUTOMAATIO-OSUUDEN KÄYTTÖÖNOTTO

Otto Berger

Opinnäytetyö
Maaliskuu 2014
Sähkötekniikka
Automaatiotekniikka

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Sähkötekniikan koulutusohjelma
Automaatiotekniikan suuntautumisvaihtoehto

BERGER, OTTO:
Turvallisuuskonseptin toteutuksen automaatio-osuuden käyttöönotto

Opinnäytetyö 66 sivua, joista liitteitä 10 sivua
Maaliskuu 2014

UPM Raflatac Oy otti koko konsernissa käyttöön uuden turvallisuuskonseptin. Tämän vuoksi tehtaalla tarvittiin henkilöä, joka tulkitsee turvallisuuteen liittyvät standardit ja muuntaa niissä esitetyt vaatimukset käytännön tasolle. Tarkoituksena oli kehittää jo olemassa olevia sekä luoda uusia turvajärjestelmiä varten sellainen turvajärjestelmän pohja, jota hieman muuntamalla saadaan luotua suoritustasoltaan erilaisia turvajärjestelmiä. Tämä pohja luotiin tekemällä esimerkkijärjestelmä yhdelle laminointikoneelle.

Toisen koneen jo olemassa olevaan järjestelmään tehtiin ensimmäisenä parannusehdotus, jolle laskettiin suoritustaso. Tämän pohjalta lähdettiin kehittämään toisen laminointikoneen kiinnirullaimelle turvajärjestelmää, jolla saavutetaan korkein tehtaalla vaadittu suoritustaso. Tälle kiinnirullaimen turvajärjestelmälle määritettiin SISTEMA-työkalua käyttäen suoritustaso, jolle kiinnirullaimelle suunnitelluilla toiminnoilla päästiin. Järjestelmä toteutettiin käytännössä ja sille tehtiin asiaankuuluvat testaukset. Testauksista ja suoritustasojen täyttymisestä luotiin dokumentaatio, joka taltioitiin.

Kiinnirullaimen turvajärjestelmä toimi hyvin. Se oli hyvä esimerkki korkean suoritustason järjestelmästä. Työssä tuotiin myös hyvin esille, miten koneturvallisuuteen liittyvät standardit saadaan sovellettua helposti käytäntöön.

Avainsanat: turva, suoritustaso, Sistema,

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Electrical Engineering
Option of Automation

BERGER, OTTO:
Commissioning the Automation Part in the Implementation of a Safety Concept

Bachelor's thesis 66 pages, appendices 10 pages
March 2014

UPM Raflatac Ltd started to use a new safety concept throughout the consolidated corporation. Therefore they needed a person in the factory who interprets the safety standards and adapts the requirements into the practical level. The idea was to develop the existing safety systems and to create new ones a base that, through slight modification, would allow creating safety systems with different performance levels. This base was created by making an example system for a laminating machine.

First, an improvement suggestion was made for the existing system of one machine, the performance level of which was calculated. Based on this, the development of a new safety system for the rewinder of another machine began, resulting in the highest performance level required in the factory. SISTEMA tool was used to determine the performance level for the safety system of this rewinder, and the level was achieved through the functions planned for the rewinder. The system was executed into practice and relevant tests were made. Testing and performance levels was documented and filed.

The safety system of the rewinder worked well and was a good example of high-performance level system. The study also highlighted how safety related standards can be easily adapted into practice was also well adduced in this work.

Key words: safety, performance level, Sistema

SISÄLLYS

LYHENTEET JA TERMIT

$MTTF_d$	vaarallinen keskimääräinen vikaantumisaika
DC	diagnostiikan kattavuus
DC_{avg}	keskimääräinen diagnostiikan kattavuus
CFF	komponenttien yhteisvikaantuminen
PL	suoritustaso
PL_r	vaadittava suoritustaso
SISTEMA	ohjelmistotyökalu koneiden turvatoimintojen suunnitteluun
B_{10d}	toimintajaksojen lkm., jolloin 10 % komponenteista vikaantuu vaarallisesti
n_{op}	keskimääräinen vuosittainen toimintajaksojen lukumäärä
PL_{low}	matalimman suoritustason omaava komponentti
N_{low}	matalimman suoritustason omaavien komponenttien lkm.
TÜV	saks. Technischer Überwachungsverein, saksalainen tarkastuslaitos
Kiinnirullain	kiinnirullainta käytetään paperirainan käärimiseen suureen konerullaan.
Laminaattori	kone, jolla laminoidaan kaksi tai useampi paperirainaa yhdeksi tuotteeksi
Karuselli	kääntölaite, jolla täysi rulla poistetaan koneen kierrosta ja uusi tyhjä rulla asetetaan tilalle

1 JOHDANTO

Opinnäytetyöni tarkoituksena oli tutkia ja etsiä turvallisuusratkaisuja laminointikoneiden, joiden rataleveys on 2 m, riskianalyyseissa määriteltyjen alueiden turvaamiseksi sähköautomaation osalta. Riskianalyysit koneiden vaara-alueista ja vaadittavista suoritustasoista määritti oma riskinarviointiryhmä.

Tehtävänäni oli tutkia minkälaisella laitteistolla ja suojauksen toteutuksella päästään sille vaadittuun suoritustasoon. Laitteiston suoritustason tutkimisessa käytin SISTEMA-ohjelmistoa, joka on työkalu turvallisuuteen liittyvien järjestelmien suoritustason määrittämiseksi. Koska koko tehdasta koskeva turvallisuuskonsepti ja siihen liittyvät suojaukset on aihealueeltaan hyvin laaja, työni käsitti parannusehdotuksen yhdelle laminointikoneen osalle sekä kokonaan uuden turvajärjestelmän suunnittelun toisen koneen osalle.

Tämän opinnäytetyön kappaleet 2 ja 3 käsittelevät standardeja SFS 5974, SFS EN ISO 13849-1 ja -2 sekä SFS-EN ISO 12100 (mistä riski koostuu, miten suoritustaso muodostuu jne.). Kappaleessa 4 esitellään SISTEMA-työkalua ja tutustutaan lyhyesti sen käyttöön. Kappaleet 5-8 sisältävät turvajärjestelmien suunnittelua sekä niiden suoritustason laskentaa SISTEMA-työkalua käyttäen.

Työ vastaa useimpiin turvajärjestelmää suunnittelevalle heränneisiin kysymyksiin, kuten: Miten suoritustaso määräytyy? Mitä vaaditaan jonkin suoritustason toteuttamiseksi? Mitä turvajärjestelmä yksinkertaisimmillaan tarkoittaa?

2 YLEISTÄ

Tässä kappaleessa käsitellään yleisiä asioita liittyen riskin arviointiin koneturvallisuudessa (SFS 12100) sekä sitä, mitä tarkoittaa vaadittava suoritustaso. Riskin arviointia sivutaan vain lyhyesti, sillä riskinarviointi ei ole tässä työssä olennaisin osa ja sen suoritti oma riskinarviointiryhmänsä. Olennaisempaa tämän työn kannalta on, miten riskianalyysin pohjalta muodostetaan koneelle tai sen osalle riskiltä suojautumiseen vaadittava laitteisto. Tämän vuoksi kappaleessa käsitellään, standardin SFS-EN ISO 13849-1 määrittämää, turvajärjestelmältä vaadittavaa tasoa.

2.1 Riskien arvioinnin ja vaaran tunnistamisen perusperiaatteet

Jokaisella automaattisesti toimivalla koneella saattaa olla osia tai alueita, joihin koskeminen tai joilla käyminen on välttämätöntä koneen toiminnan kannalta. Näihin osiin koskeminen tai alueilla käyminen tulisi olla turvallista eikä siitä saisi aiheutua kohtuutonta vaara koneen käyttäjälle. Niinpä jokaiselle tällaiselle osalle tai useammasta osasta koostuvalle alueelle tulisi määrittää riski altistua kyseiselle vaaralle. "Riskin arviointi on sarja loogisesti eteneviä vaiheita, jotka tekevät mahdolliseksi järjestelmällisen koneisiin liittyvien riskien analysoinnin ja niiden merkityksen arvioinnin." (SFS-EN ISO 12100 2010, 28.)

Riskin arvioimiseksi ja sen pienentämiseksi on kehitetty hyviä työkaluja. Helpoiten käytettäviä työkaluja ovat vuokaavio-malliset työkalut, joissa riskiä arvioidaan vaihe vaiheelta (ks. liite 1). Riskin arviointia ja sen pienentämistä koskevat kaaviot on esitetty standardin SFS 12100 alussa riskiä arvioivan henkilön/henkilöiden sekä riskin pienentämiseksi työskentelevän turvallisuussuunnittelijan näkökulmasta (ks. liite 2). Näissä kaavioissa lähestytään riskin tunnistusta ja pienentämisprosessia lohko kerrallaan. Lohkosta toiseen siirtyminen tapahtuu aina "kyllä"- tai "ei"-ehdon mukaan ja kuljettavasta polusta riippuen päädytään joko kaavion loppuun ja riskin toteamiseen tai takaisin lähelle alkua.

Kun koneen tai sen osan toimintaan liittyvä riski ja vaara on tunnistettu, päästään määrittämään vaaralta suojautumiseksi vaadittava turvatoiminnon suoritus- eli PL_r (Performance Level) -taso.

2.2 Vaadittavan suoritus- eli PL_r-tason määrittäminen

Jokaiselle turvatoiminnolle määritetään oma vaadittava suoritustasonsa, jotka jakautuvat viiteen eri luokkaan PL_r a, b, c, d ja e. Näistä viidestä luokasta a on kevyin ja vaatii vähiten turvatoimintoja. Vastaavasti e-luokka on vaativin luokka, jonka toteuttamiseksi vaaditaan turvatoimintoihin suunniteltuja komponentteja ja mutkikkaampia järjestelmiä.

Käytännössä PL_r-taso määräytyy kolmen perusmuuttujan perusteella: vaaratilanteesta aihetuvan vamman vakavuus S, vaaralle alistumisen taajuus ja/tai kesto F sekä mahdollisuus välttää kyseinen vaara P. Nämä kolme muuttujaa jaetaan vielä kahteen ryhmään seuraavasti:

S1 = lievä vamma (tavallisesti palautuva)

S2 = vakava vamma (palautumaton vamma tai kuolema)

F1 = harvoin...toisinaan ja/tai lyhyt aika altistumiselle

F2 = toistuvasti...jatkuvasti ja/tai pitkä altistumisaika

P1 = mahdollista välttää vaara tietyissä olosuhteissa

P2 = tuskin mahdollista välttää vaaraa

(SFS-EN ISO 13849-1 2008, 100.)

UPM Rafalatac Oy käyttää lisäksi neljää riskiparametria standardin SFS-EN 1050 mukaisesti, joista johdetaan Excel-taulukossa edellä mainitut parametrit. Standardin määrittämät parametrit ja niiden selitykset on esitetty liitteessä 3. SFS-EN 1050:ssä esiintyvät parametrit ovat laajuudeltansa enemmän suuntaa antavat, sillä niissä vaihtoehtoja riskin arvioimiseksi tapahtumaa kohti on enemmän. Neljästä riskiä arvioivasta tekijästä muodostuu vaaralle riski, joka määritetään seuraavasti:

$R = S*E*T*H$, missä (1)

R = riski

S = tapaturman seuraukset

E = tapahtuman todennäköisyys

T = altistumisen taajuus

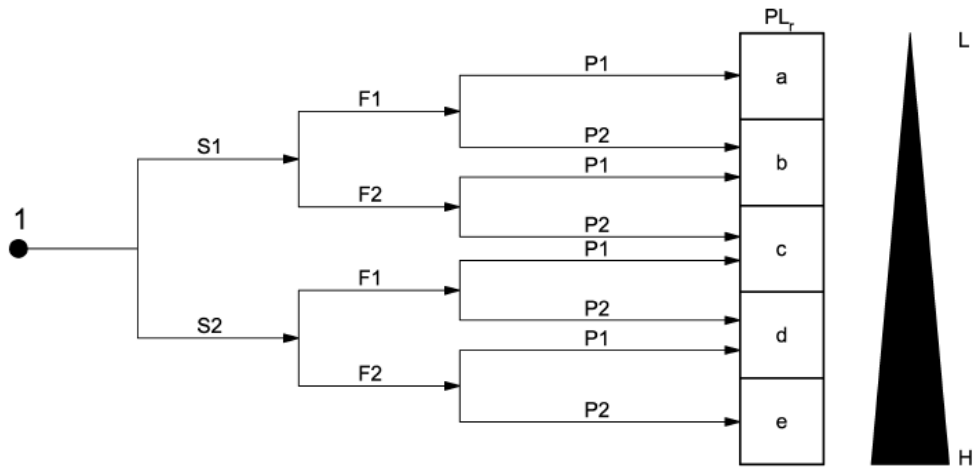
H = tapaturmalle altistuvien henkilöiden lukumäärä

Jotta näistä neljästä parametrista päästäisiin SFS-EN ISO 13849-1:ssa mainittuihin kolmeen parametriin ja niiden kautta vaadittavan suoritustason määritykseen, täytyy nämä neljä parametria sovittaa taulukon 1 mukaisesti.

TAULUKKO 1. Riskiparametrien muuntaminen

Parametrien muuntaminen			
SFS-EN- 1050	**Lukuarvo**	**SFS-EN ISO 13849-1**	**Lukuarvo**
S	< tai = 2	S	1
S	> tai = 4	S	2
T	< tai = 0,5	F	1
T	> tai = 1	F	2
E	< tai = 2	P	1
E	> tai = 2	P	2

Kun vaaran riskiä ilmaisevat perusmuuttujat S, F ja P on määritetty, päästään itse vaadittavan suoritustason määrittämiseen. PL_r-tason määrittäminen on helppoa siihen suunnitellun kaavion perusteella (kuvio 1). Sama kaavio esiintyy myös myöhemmin esiteltävässä SISTEMA-ohjelmistossa, kun määritetään turvallisuusfunktion vaadittavaa suoritustasoa. Kaaviota kuljetaan vasemmalta (pisteestä 1) oikealle, jolloin päädytään lopulta, kuljetusta polusta riippuen, riskiä vastaan vaadittavaan suoritustasoon.



KUVIO 1. PL_r-tason määritys (SFS-EN ISO 13849-1 2008, 100)

Kun koneelle tai sen osalle on määritelty edellä mainittujen ohjeiden perusteella suojaukselta vaadittava suoritustaso, aloitetaan suunnitella miten tähän suoritustasoon päästään. Suojaustoiminto voi olla mekaaninen tai sähköinen suojaus riippuen suojattavasta vaara-alueesta ja vaadittavasta suoritustasosta PL_r. Käytettiin sitten mekaanista tai sähköistä suojausta, sen tulee täyttää tietty suoritustaso PL. Seuraavassa kappaleessa on käsitelty laitteiston suoritustason muodostumista.

3 LAITTEISTON SUORITUSTASON, PL, MUODOSTUMINEN

Standardissa ISO 13849-1 on esitetty näkökohtia, joiden perusteella arvioidaan laitteiston kykyä toteuttaa jokin tietty turvatoiminto eli määritetään laitteiston PL-taso. Näkökulmat liittyvät yhtä turvatoimintoa koskevan koko suojauksen sekä yksittäisten komponenttien luotettavuuden arviointiin. Jokaisen osajärjestelmän suoritustasoa arvioitaessa tulisi huomioida ainakin seuraavat standardissa esitetyt näkökohdat:

- vaarallinen keskimääräinen vikaantumisaika, $MTTF_d$
- diagnostiikan kattavuus, DC
- komponenttien yhteisvikaantuminen, CCF
- järjestelmän rakenne
- turvatoimintojen käyttäytyminen vikatilanteessa/-tilanteissa
- turvatoimintoja toteuttava ohjelmisto
- järjestelmän systemaattinen vikaantuminen
- turvatoiminnon toteutuminen ennakoitavissa olevissa ympäristöolosuhteissa.

(SFS-EN ISO 13849-1 2008, 42.)

Näistä näkökohdista $MTTF_d$:n, DC:n ja CCF:n arviointia helpottaa niiden määrittämiseen luodut valmiit ohjelmistot. Tässä työssä on käsitelty SISTEMA-ohjelmistoa, jota käytin itse UPM Raflatacilla turvallisuusjärjestelmien suoritustasojen määrittämiseen. Seuraavassa on esitelty tarkemmin miten edellä mainitut näkökohdat määritetään.

3.1 Vaarallinen keskimääräinen vikaantumisaika, $MTTF_d$

Kullekin osajärjestelmän kanavalle voidaan määrittää vaarallinen keskimääräinen vikaantumisaika, jolla on mahdollista olla kolme eri tasoa. Koska vaarallinen vikaantumisaika, joka määritetään vuosina, voi saavuttaa suuria arvoja, on loogisempaa määrittää sille todellisempi maksimiaika. Tämä aika on standardissa 13849-1 määritetty 100 vuoteen. $MTTF_d$-arvojen kolme tasoa määritetään taulukon kaksi mukaisesti.

TAULUKKO 2. Kanavan vaarallinen keskimääräinen vikaantumisaika ($MTTF_d$), (SFS-EN ISO 13849-1 2008, 46)

	$MTTF_d$
Kunkin kanavan merkintä	**Kunkin kanavan vaihteluväli**
matala (low)	3 vuotta ≤ $MTTF_d$ < 10 vuotta
keskimääräinen (medium)	10 vuotta ≤ $MTTF_d$ < 30 vuotta
korkea (high)	30 vuotta ≤ $MTTF_d$ ≤ 100 vuotta

HUOM. 1 Kunkin kanavan $MTTF_d$ -arvojen vaihteluvälien valinta perustuu nykytekniikan mukaisista kenttähavainnoista saatuihin vikataajuuksiin ja ne muodostavat tietyntyyppisen logaritmisen asteikon, joka sopii logaritmiseen suoritustason asteikkoon. Todellisten turvallisuuteen liittyvien ohjausjärjestelmän osien jokaisen kanavan $MTTF_d$ -arvoja, jotka ovat alle kolme vuotta, ei oleteta esiintyvän, koska tämä tarkoittasi, että yhden vuoden kuluttua noin 30 % markkinoilla olevista järjestelmistä vikaantuisivat ja ne pitäisi korvata. Minkään kanavan $MTTF_d$ -arvoa yli 100 vuotta ei hyväksytä, koska suuria riskejä varten olevat turvallisuuteen liittyvät ohjausjärjestelmän osat eivät saisi riippua yksistään komponenttien luotettavuudesta. Turvallisuuteen liittyvien ohjausjärjestelmän osien vahvistamiseksi systemaattisia ja satunnaisia vikaantumisia vastaan olisi vaadittava täydentäviä keinoja kuten redundanssia ja testausta. Käytännön syistä vaihteluvälit rajoitetaan kolmeen. Jokaisen kanavan $MTTF_d$ -arvon rajoittaminen enintään 100 vuoteen koskee turvallisuuteen liittyvien ohjausjärjestelmän osien yhtä kanavaa, jotka toteuttavat turvatoiminnon. Korkeampia $MTTF_d$ -arvoja voidaan käyttää yksittäisille komponenteille (ks. taulukko D.1).

HUOM. 2 Tässä taulukossa esitettävien rajojen tarkkuuden oletetaan olevan 5 %.

Yksittäisen kanavan keskimääräinen vaarallisen vikaantumisen aika määritetään kanavan yksittäisten komponenttien $MTTF_d$-arvojen summana. Yksittäisen komponentin vaarallisen vikaantumisajan määrittäminen tapahtuu seuraavassa standardin SFS-EN ISO 13849-1 (2008) osoittamassa järjestyksessä:

Tapa 1.

Valmistaja on antanut valmiiksi yksittäiselle komponentille $MTTF_d$-arvon, jolloin käytetään sitä. Valmistaja saattaa ilmoittaa komponentille myös B_{10d} -arvon. Tämä on komponentin keskimääräinen toimintajaksojen lukumäärä, jolloin 10 % komponenteista on vikaantunut vaarallisesti.

Tapa 2.

$MTTF_d$-arvo voidaan määrittää laskemalla se. Tarkemmat laskutoimitukset ja menetelmät on esitetty standardin 13849-1 liitteissä C ja D. Liitteen C taulukoissa C.2-C.7 on esitetty myös joitakin tyypillisiä $MTTF_d$-arvoja yleisimmille komponenteille. Alla on kuitenkin joitakin peruslaskentamenetelmiä, kun tiedetään komponentista joitakin muita tietoja kuin suoraan $MTTF_d$-arvo.

B_{10d} -arvosta määritetään $MTTF_d$-arvo seuraavasti:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}, \text{ missä} \qquad (2)$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cycl\ jakso}}$$, missä (3)

n_{op} = keskimääräinen vuosittainen toimintajaksojen lukumäärä

h_{op} = keskimääräinen toiminta-aika, tuntia päivässä

d_{op} = keskimääräinen toiminta-aika, päivää vuodessa

$t_{cycl\ jakso}$ = komponentin kahden peräkkäisen toimintajakson alkamisajankohdan välinen keskimääräinen aikaväli (esim. venttiilin avaaminen), sekuntia per toimijakso

(SFS EN-ISO 13849-1 2008, 110.)

Tai vaihtoehtoisesti mikäli tiedetään aika jolloin 10 % komponenteista on vikaantunut (T_{10d}) voidaan määrittää keskimääräinen vaarallinen vikaantumisaika seuraavasti:

$$MTTF_d = \frac{T_{10d}}{0{,}1}$$ (4)

T_{10d} -arvo voidaan myös laskea, kun tiedetään B_{10d}:

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$ (5)

(SFS-EN ISO 13849 2008, 110, 112.)

Tapa 3.

Käytetään lukuarvoa 10 vuotta mikäli mitään yllä olevista menetelmistä ei ole mahdollista toteuttaa esimerkiksi komponentista ei ole saatavissa mitään tietoja $MTTF_d$-arvon laskemiseksi.

3.2 Diagnostiikan kattavuus, DC

Jokaisella kanavalla on oma diagnostiikan kattavuutensa eli tarkoittaa käytännössä sitä onko kyseisen kanavan toiminnasta saatavissa tietoa (esimerkiksi takasinkytkentä releeltä). DC määritellään neljällä tasolla, jotka on esitetty taulukossa kolme.

TAULUKKO 3. Diagnostiikan kattavuus, DC (SFS-EN ISO 13849-1 2008, 48)

DC	
Merkintä	**Vaihtelualue**
nolla (none)	DC < 60 %
matala (low)	60 % ≤ DC < 90 %
keskimääräinen (medium)	90 % ≤ DC < 99 %
korkea (high)	99 % ≤ DC

HUOM. 1 Useasta osasta koostuvan turvallisuuteen liittyvän ohjausjärjestelmän osan diagnostiikan kattavuudelle (DC) käytetään kuvassa 5, kohdassa 6 ja liitteessä E.2 keskimääräistä diagnostiikan kattavuutta (DC_{avg}).

HUOM. 2 Diagnostiikan kattavuudelle valitut arvojen vaihteluvälit perustuvat avainarvoihin 60 %, 90 % ja 99 %, joita käytetään myös muissa standardeissa (esim. IEC 61508), joissa käsitellään diagnostiikan kattavuuden testauksia. Tutkimukset osittavat, että pikemminkin (1 – DC) kuin itse DC, on testauksen tehokkuudelle ominainen mitta. Avainarvoja 60 %, 90 % ja 99 % vastaavat (1 – DC) arvot muodostavat tietyntyyppisen logaritmisen asteikon, joka sopii logaritmiseen suoritustason asteikkoon. DC-arvoa 60 % pienemmällä arvolla on vain vähäinen merkitys testatun järjestelmän luotettavuuteen ja siksi se merkitään "nolla (none)". DC-arvoa 99 % suurempaa arvoa on hyvin vaikea saavuttaa monimutkaisilla järjestelmillä. Käytännön syistä vaihteluvälit rajoitetaan neljään. Tässä taulukossa esitettävien rajojen tarkkuuden oletetaan olevan 5 %.

Diagnostiikan kattavuuden ja keskimääräisen vaarallisen vikaantumisajan perusteella voidaan määrittää jo kanavan suoritustaso, kun tiedetään mihin luokkaan (ks. kappale 3.4) kanava kuuluu. Diagnostiikan kattavuutta voidaan määrittää tekemällä järjestelmälle vika- ja vaikutusanalyyseja eli tutkimalla mitä toimintoja turvajärjestelmässä eri viat aiheuttavat. Standardin SFS-EN ISO 13849-1 (2008) liitteessä E on taulukoituna useita esimerkkejä diagnostiikan kattavuudesta erilaisille tulo- ja lähtöyksiköille.

Koska yhdessä turvallisuusjärjestelmässä voi olla useita menetelmiä vikojen diagnostisoimiseksi ja niillä kaikilla on omat diagnostiikan kattavuutensa, täytyy turvatoimintoa suorittavien ohjausjärjestelmän osien kokonaisuudelle laskea keskimääräinen diagnostiikan kattavuus DC_{avg}. Tämä arvo saadaan paljastuneiden vaarallisten vikaantumisten vikaantumistaajuuden ja kaikkien vaarallisten vikaantumisten vikaantumistaajuuden suhteena:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \quad (6)$$

(SFS-EN ISO 13849-1 2008, 128)

3.3 Yhteisvikaantuminen, CCF

Edellä esiteltyjen diagnostiikan kattavuuden ja vaarallisen keskimääräisen vikaantumisajan lisäksi tulisi turvallisuuteen liittyvien ohjausjärjestelmän osien suoritustasoa arvioitaessa ottaa huomioon myös kunkin osan yhteisvikaantumisen mahdollisuus. Yhteisvikaantumisen estämiseksi tehtävät toimenpiteet antureille, toimilaitteille ja logiikalle on esitetty standardissa IEC 61508-6:2000 liitteessä D. Yhteisvikaantumisen analysoimiseksi on tehty taulukko, jossa kukin ohjausjärjestelmän osa käydään läpi ja pisteytetään liitteen neljä mukaisesti.

Pisteytys tapahtuu siten, että jokaisesta kohdasta saa joko täydet pisteet tai ei mitään. Kuten liitteestä neljä ilmenee, pisteytysprosessin maksimipistemäärä on 100 ja minimi on 65 pistettä. Jos turvajärjestelmän osa saavuttaa 65 pistettä tai enemmän, sen yhteisvikaantumisen estämiseksi tehdyt toimenpiteet ovat riittävät. Mikäli jäädään kuitenkin alle tämän pistemäärän, tarvitsee tehdä lisätoimenpiteitä liittyen liitteen neljä kohtiin 1-6.

3.4 Luokat ja niiden merkitys

Jokainen turvallisuuteen liittyvän ohjausjärjestelmän osa kuuluu johonkin luokkaan. Luokkia on kaiken kaikkiaan viisi: B, 1, 2, 3 ja 4. Näitä viittä luokkaa käytetään tietyn suoritustason saavuttamiseksi. Suoritustasoltaan matalin luokka on B ja vastaavasti paras luokka on neljä. Luokat ovat perusmuuttujia ja ne määräytyvät käytännössä turvallisuusjärjestelmän osassa käytettyjen komponenttien laadun sekä niillä muodostetun kytkennän (onko esimerkiksi diagnostiikkaa vai ei) perusteella.

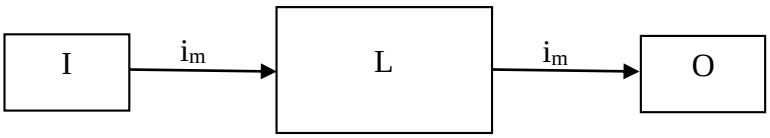
3.4.1 Luokka B

Alin luokka, jota kutsutaan myös perusluokaksi. Luokan vaatimuksena on, että käytetyt komponentit sekä niiden kytkennät täyttävät asiaankuuluvat standardit. Niiden tulee myös kestää seuraavat perusmuuttujat:

- odotettavissa olevat käyttökuormitukset
- käsiteltävien aineiden vaikutukset
- muut merkittävät ulkoiset vaikutukset, kuten tärinä, sähkömagneettiset häiriöt yms.

(SFS-EN ISO 13849-1 2008, 76.)

Tähän luokkaan kuuluva järjestelmä ei sisällä diagnostiikan kattavuutta (DC). Kunkin kanavan $MTTF_d$-arvo voi olla pieni tai keskimääräinen. Myöskään kanavan/kanavien yhteisvikaantumista (CCF) ei tarvitse ottaa huomioon. Näillä ehdoilla voidaan siis B luokkaan kuuluvalla järjestelmällä saavuttaa suoritustaso PL b. Järjestelmän rakenne on esitetty kuviossa 2.



i_m = kytkentävälineet
I = tuloyksikkö (esim. anturi)
L = logiikka
O = lähtöyksikkö

KUVIO 2. Luokan B rakenne (SFS-EN ISO 13849-1 2008, 78)

3.4.2 Luokka 1

Luokassa 1 tulee käyttää hyvin koeteltuja komponentteja sekä turvallisuusperiaatteita (ks. ISO 13849-2). Kun puhutaan turvallisuuteen liittyvästä hyvin koetellusta komponentista, tulee kyseisen komponentin täyttää seuraavat ehdot:

a) komponenttia on käytetty aiemmin laajasti ja siitä on hyviä kokemuksia vastaavissa järjestelmissä
b) komponentin valmistaja on valmistanut ja todentanut komponentin siten, että se on sopiva ja luotettava käytettäväksi turvallisuuteen liittyvissä sovelluksissa.

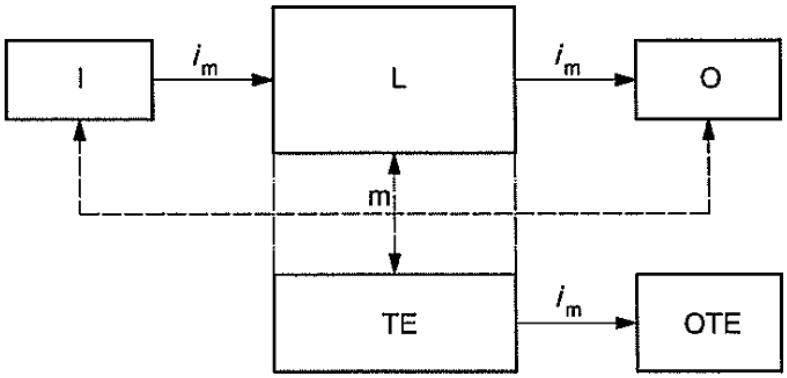
Mikäli käytetään uudentyyppisiä komponentteja, niiden voidaan todeta olevan hyvin koeteltuja mikäli ne täyttävät kohdan b ehdot. Luokassa 1 vaadittava $MTTF_d$-arvo on oltava korkea (≥ 30 vuotta). Myöskään tässä yhteisvikaantumista tai diagnostiikkaa ei tarvitse huomioida sillä luokan 1 järjestelmät ovat tyypillisesti yksikanavaisia. Suurin luokalla yksi saavutettava suoritustaso on PL c ja tämän luokan mukaisen järjestelmän rakenne on vastaava kuin luokan B (ks. kuvio 2). (SFS-EN ISO 13849-1 2008, 78.

3.4.3 Luokka 2

Myös luokassa 2 noudatetaan luokan B vaatimuksia sekä käytetään luokassa 1 mainittuja hyvin koeteltuja turvallisuusperiaatteita. Näiden kahden kohdan lisäksi tulee luokassa 2 koneen ohjausjärjestelmän tarkistaa turvallisuuteen liittyvät ohjausjärjestelmän osat säännöllisin väliajoin (diagnostiikka). Tarkistuksen tulee tapahtua ainakin seuraavissa:
- koneen käynnistyksen yhteydessä
- ennen minkään vaaratilanteen alkamista (liikkeiden tai uuden toimijakson käynnistyminen)
- ja/tai määräajoin koneen toiminnan aikana, mikäli tarpeellista riskin arvioinnin ja kyseessä olevan käyttötoiminnan perusteella.
(SFS-EN ISO 13489-1 2008, 80.)

Tarkistus voi olla automaattinen ja sen tehtävänä on sallia koneen käyttötoiminta (mikäli vikoja ei ole ilmaantunut) tai muodostettava lähtösignaali mikäli vika paljastuu. Lähtösignaali käynnistää tarvittavan ohjaustoimenpiteen, jolla koneen siirtyminen turvalliseen tilaan aloitetaan. Jos tämä ei ole mahdollista, täytyy lähtösignaalin saada aikaan varoitus, että turvalliseen tilaan ei ole päästy.

Tutkittaessa luokan kaksi turvallisuusjärjestelmän DC_{avg} - ja $MTTF_d$ –arvoja, tulee ottaa huomioon vain toiminnalliset kanavat I,L ja O (kuvio 3). Tarkistukseen liittyvän kanavan lohkoja TE ja OTE ei tarvitse huomioida (ks. kuvio 3). Tämän luokan DC_{avg} -tason on oltava vähintään matala ja $MTTF_d$ -tason matala - korkea riippuen vaadittavasta suoritustasosta. Yhteisvikaantumista (CCF) vastaan on suojauduttava. Suurin saavutettava suoritustaso luokassa 2 on PL d. Kuviossa 3 esitetyt katkoviivat kuvaavat käytännössä kohtuudella mahdollista vikojen paljastamista. (SFS-EN ISO 13849-1 2008, 80.)



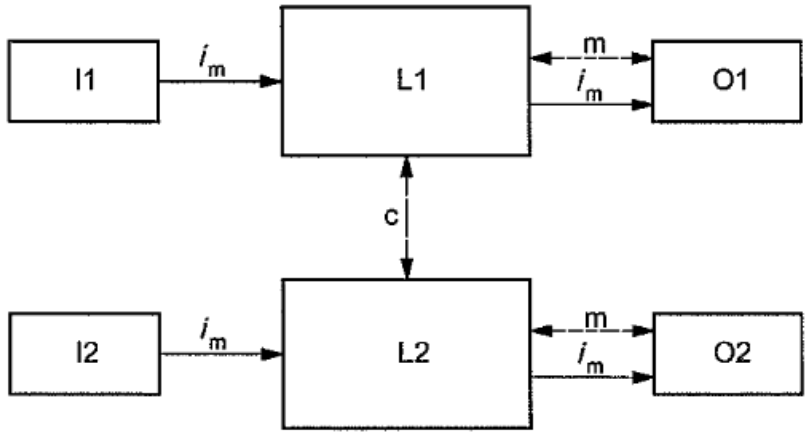
i_m = kytkentävälineet
I = tuloyksikkö (esim. anturi)
L = logiikka
O = lähtöyksikkö
m = valvonta
TE = testauslaitteisto
OTE = testauslaitteiston lähdöt

KUVIO 3. Luokan 2 rakenne (SFS-EN ISO 13849-1 2008, 82)

3.4.4 Luokka 3

Luokassa 3 noudatetaan luokassa B esitettyjen periaatteiden lisäksi hyvin koeteltuja turvallisuusperiaatteita. Näiden lisäksi luokassa 3 yksittäisen vian ilmeneminen ei johda turvallisuustoiminnon menettämiseen (luokassa 2 yksittäisen vian ilmeneminen saa johtaa turvatoiminnon menettämiseen). Yksittäisen vian on paljastuttava turvatoiminnon vaateen yhteydessä tai mahdollisesti ennen sitä, mikäli tämä on kohtuudella mahdollista.

Luokan 2 tavoin myös luokassa 3 keskimääräisen diagnostiikan kattavuuden tulisi olla tasoa matala (vähintään) ja vaarallisen keskimääräisen vikaantumisajan matala-korkea (riippuu PL_r tasosta). Myös yhteisvikaantumista vastaan on suojauduttava. Vaikka luokassa kolme edellytetään yksittäisen vian paljastumista, tämä ei tarkoita, että kaikki viat paljastuisivat. Näiden paljastumattomien vikojen kertyminen saattaa johtaa vaaratilanteeseen. Luokan 3 tyyppinen turvajärjestelmän rakenne on kaksikanavainen (ks. kuvio 4). Kuviossa 4 katkoviivat kuvaavat kohtuudella mahdollista vikojen paljastamista.



i_m = kytkentävälineet
c = ristiinvalvonta
I1, I2 = tuloyksikkö (esim. anturi)
L1, L2 = logiikat
O1, O2 = lähtöyksikkö (esim. pääkontaktori)
m = valvonta

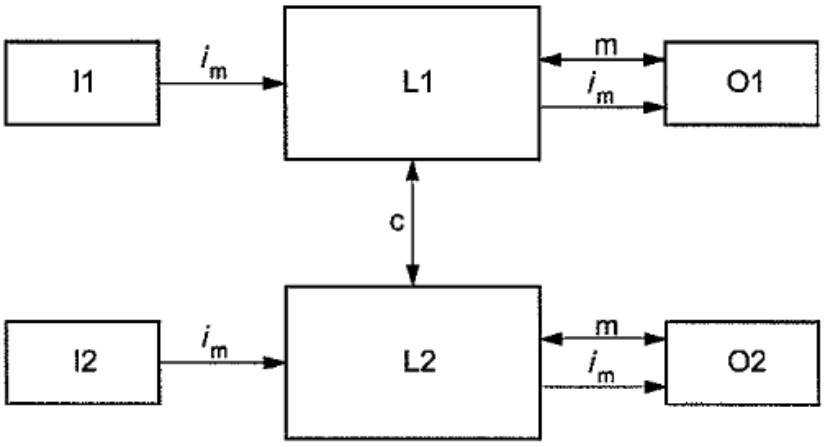
KUVIO 4. Luokan 3 rakenne (SFS-EN ISO 13849-1 2008, 84)

3.4.5 Luokka 4

Viimeinen ja korkein luokka vaatimuksiltaan ja mahdolliselta suoritustasoltaan on luokka 4. Tähän sovelletaan luokan B mukaisia vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita. Näiden lisäksi luokan 4 turvallisuusjärjestelmän osat on suunniteltava siten, että yksittäinen vika ei johda järjestelmän missään osassa turvatoiminnon menettämiseen. Vian tulee myös paljastua aina seuraavan vaateen yhteydessä tai ennen sitä (koneen käynnistys tai toiminnon lopussa). Mikäli tämä vikojen paljastaminen ei ole mahdollista, paljastumattomien vikojen kertyminen ei saa johtaa turvatoiminnon menetykseen. Lisäksi edellytetään, että vikojen tulee paljastua ajoissa, jotta turvatoimintoa ei menetetä. (SFS-EN ISO 13849-1 2008, 84.)

Luokassa neljä tulee DC_{avg} -tason olla korkea. Lisäksi kunkin kahdennetun kanavan $MTTF_d$ -tason on oltava korkea. Yhteisvikaantumista vastaan on suojauduttava. Luokat 3 ja 4 eroavat toisistaan juuri siinä, että luokassa 4 edellytetään korkeampaa keskimääräistä

diagnostiikan kattavuutta sekä kanavien korkeata vaarallista keskimääräistä vikaantumisaikaa. Korkeaan diagnostiikan tasoon voidaan päästä käytännössä jo sillä, että tutkitaan kahden eri vian muodostamaa yhdistelmää. Luokan 4 mukaisen järjestelmän rakenne vastaa muuten luokan 3 mukaisen järjestelmän rakennetta, mutta siinä diagnostiikan kattavuus on suurempi. Tämä on kuvattu kuviossa 5 valvontatoimintojen yhtenäisinä viivoina (kuviossa 4 katkoviivoina).



i_m = kytkentävälineet
c = ristiinvalvonta
I1, I2 = tuloyksikkö (esim. anturi)
L1, L2 = logiikat
O1, O2 = lähtöyksikkö (esim. pääkontaktori)
m = valvonta

KUVIO 5. Luokan 4 rakenne (SFS-EN ISO 13849-1 2008, 86)

3.5 Turvallisuuteen liittyvän järjestelmän kokonaissuoritustason saavuttaminen

Yhteen turvallisuusjärjestelmään saattaa kuulua N kappaletta eri osia, joilla on eri suoritustasot. Näitä suoritustasoja voidaan nimetä muuttujalla PL_i. Järjestelmässä matalimman suoritustason omaavilla osilla on sama suoritustaso PL_{low}, joita voi olla yksi tai useampi ja niitä nimetään muuttujalla N_{low}. Näiden PL_{low}-arvon omaavilla osilla on suuri vaikutus koko järjestelmän suoritustasoon taulukon 4 mukaisesti.

TAULUKKO 4. Suoritustasot turvallisuusjärjestelmä kokonaisuudelle (SFS-EN ISO 13849-1 2008, 92)

PL_{low}	**N_{low}**	⇨	**PL**
a	> 3	⇨	Ei mitään, ei sallittu
	≤ 3	⇨	a
b	> 2	⇨	a
	≤ 2	⇨	b
c	> 2	⇨	b
	≤ 2	⇨	c
d	> 3	⇨	c
	≤ 3	⇨	d
e	> 3	⇨	d
	≤ 3	⇨	e
HUOM. Tähän taulukkoon lasketut arvot perustuvat luotettavuusarvoihin kunkin suoritustason keskipisteessä			

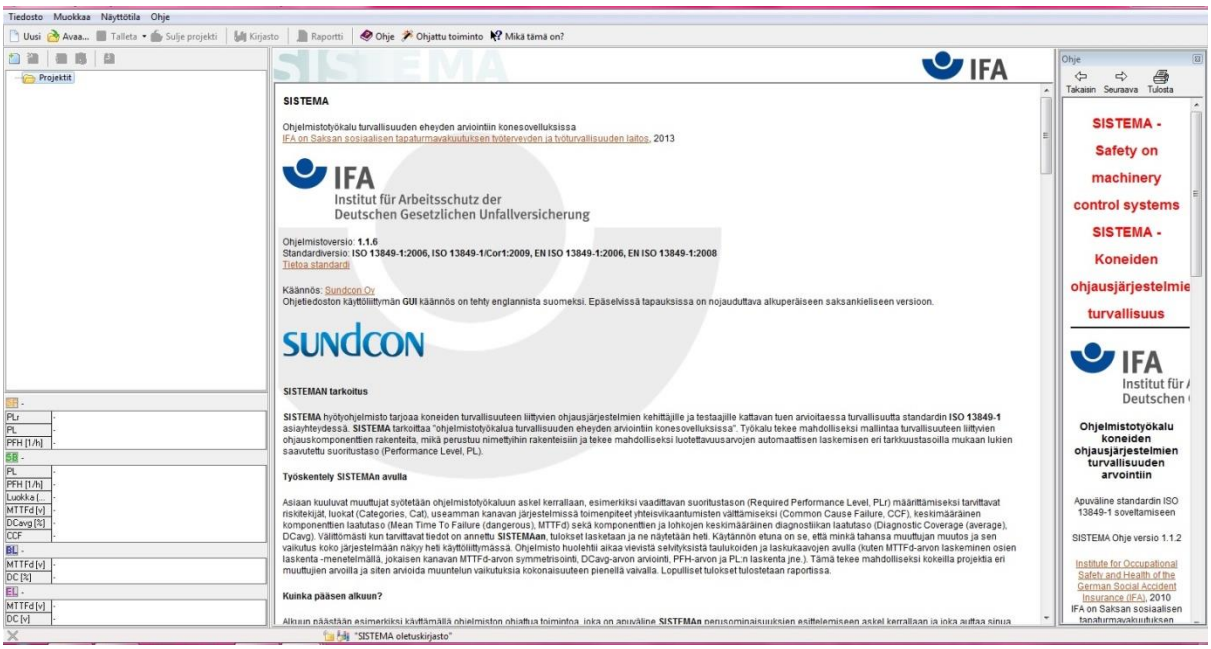
Taulukosta 4 nähdään, että esimerkiksi järjestelmän, johon kuuluu yli kaksi osaa, joiden suoritustaso on PL c, kokonaissuoritustaso putoaa tasolle PL b. Laskettaessa siis järjestelmäkokonaisuutta, on jokaisen siihen kuuluvan osan suoritustaso huomioitava erikseen, jotta koko järjestelmän suoritustaso saataisiin laskettua oikein. Kappaleessa 4 esiteltävä SISTEMA-ohjelmistotyökalu tekee tämän automaattisesti, joten käyttäjä saa suoraan tietää turvajärjestelmän oikean PL-tason.

4 SISTEMA-OHJELMISTOTYÖKALU

SISTEMA on työkalu, jota käytetään koneiden turvallisuusjärjestelmien suunnitteluun. Ohjelma auttaa käyttäjää oikeiden komponenttien valinnassa, jotta luotava turvallisuusjärjestelmä täyttäisi riskikartoituksessa määritetyt vaadittavat suojatoimenpiteet ja täyttäisi vaaditun suoritustason (ks. kpl 2.2). SISTEMA on ilmaisohjelmisto ja on ladattavissa osoitteesta http://www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp. Ohjelma on käännetty usealle kielelle ja on saatavissa myös suomeksi. Suomenkielisestä käännöksestä vastaa Sundcon Oy.

SISTEMA on luotu Saksassa/IFA:ssa ja se perustuu kokonaisuudessaan standardiin SFS-EN ISO 13849-1. Ohjelmalla voidaan optimoida turvallisuusjärjestelmiä ja se laskee automaattisesti Markovin-malliin perustuvat luotettavuustekniset mallit. SISTEMAAN on saatavilla myös lukuisten eri valmistajien (mm. ABB, Phoenix, Omron) luomia komponenttikirjastoja, jotka helpottavat järjestelmien luontia. (Sundcon Oy 2014.)

Seuraavassa on esitelty lyhyesti SISTEMA:n perustoimintoja sekä turvallisuusjärjestelmän mallintamista. Tarkempia ohjeita työkalun käyttöön löytyy netistä (SISTEMA Cookbooks) tai ohjelman omasta apu-toiminnosta.



KUVA 1. SISTEMA-ohjelmiston aloitusnäkymä

4.1 SISTEMA-projektit

SISTEMA:ssa projektit ovat ohjelman ylin taso. Omassa työssäni projektit käsittävät yhden laminointikoneen osan turva-alueen turvajärjestelmät, esimerkiksi myöhemmin esiteltävän CM1:n kiinnirullaimen turva-alue on yksi projekti. Yhdestä projektista saadaan tulostettua SISTEMA:n automaattisesti laatima raportti. Projektia merkitään ohjelmistossa punaisin kirjoitetuin kirjaimin PR.

Projekti-ikkunassa määritetään mm. projektin nimi, tekijän nimi, koneen vaarakohta ja siihen liittyvien dokumentaation sekä standardien hakemisto-kansiot. Projekti jakautuu pienempiin osiin, jotka taas jakautuvat pienempiin osiin. Projektin tasot ja merkinnät ovat seuraavat ylimmästä tasosta alaspäin lueteltuna:

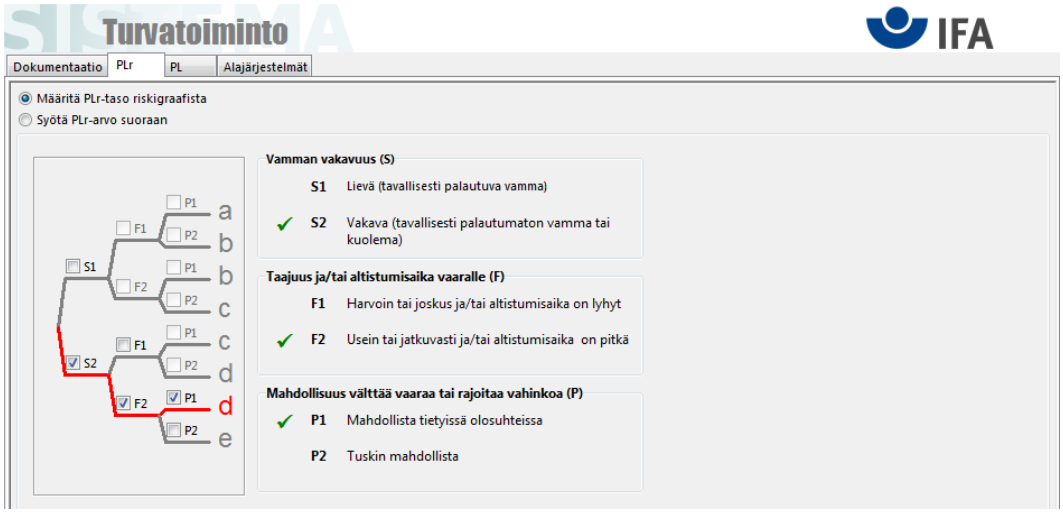
PR = projekti
SF = Safety Function eli turvatoiminto
SB = Subsystem eli alajärjestelmä
CH = Channel eli kanava
TE = Test eli testauskanava (näkyvissä riippuen luokasta)
BL = Block eli lohko
EL = Element eli elementti

Ensimmäisenä projektiin (turva-alueeseen) lähdetään muodostamaan yllä olevan kaavion mukaisesti siis turvatoimintoja, joiden tarkoituksena on suojata koneen käyttäjää joltakin tietyltä koneen osalta tai toiminnalta

4.2 Turvatoiminto

Yhdellä turva-alueella voi olla useita turvatoimintoja riippuen alueen mahdollisista vaaroista. Dokumentaatio-välilehdellä määritellään turvatoiminnolle nimi sekä alasvetovalikosta tyyppi, esimerkiksi passivointitoiminto. Dokumentaatiossa myös kerrotaan mikä laukaisee turvatoiminnon ja mikä on sen reaktio. Siellä myös määritetään mikä on koneen turvallinen tila turvatoiminnon lauettua.

Jokaiselle turvatoiminnolle määritellään joko riskigraafista (ks. kuva 2) tai annetaan suoraan (riskinarviointiryhmän määrittämä) vaadittava suoritustaso. Se mihin suoritustasoon PL turvatoiminnolla päästään riippuu alajärjestelmistä. Alajärjestelmät-välilehdeltä lisätään turvatoimintoon alajärjestelmiä.



KUVA 2. SISTEMA-näkymä turvatoiminnon PL_r-tason määrityksestä

4.3 Alajärjestelmä

Alajärjestelmä voidaan luoda turvatoiminnosta joko luomalla suoraan uusi tai valitsemalla kirjastosta jonkun valmistajan määrittämä, yhtä alajärjestelmää vastaava, komponentti esimerkiksi turvarele. Valittaessa valmistajan määrittämä komponentti, tulee alajärjestelmälle automaattisesti jokin suoritustaso ja luokka, johon kyseisellä komponentilla päästään. Mikäli kuitenkin joudutaan luomaan uusi alajärjestelmä, tarvitsee siellä määrittää kaikki erikseen.

Dokumentaatio-välilehdellä nimetään alajärjestelmä ja annetaan siihen liittyvää kuvausta. PL-välilehdellä alajärjestelmälle voidaan joko suoraan kirjoittaa vaadittava suoritustaso tai määrittää se lohkojen perusteella. Luokka-välilehdellä määritetään alajärjestelmän luokka (ks. kpl 3.4). Luokan valinta vaikuttaa alajärjestelmän rakenteeseen (onko testausta, onko kaksi- vai yksikanavainen). Valinta tapahtuu alasvetovalikosta, jossa on esitetty kaikki viisi luokkaa lähes vastaavasti, kuin ne on esitetty standardin SFS-EN ISO 13849-1 (2008) taulukossa 10. Samalla välilehdellä kysytään myös alajärjestelmän ja sen

komponenttien hyvyydestä. Luokan valintaan liittyen on myös mahdollista esittää dokumentaatiota tai johtopäätöksiä.

Alajärjestelmän $MTTF_d$-arvo voidaan määrittää joko suoraan tai lohkojen $MTTF_d$-arvoista. Lohkoja luodaan lisää alajärjestelmän Lohkot-välilehdeltä. Suoraan määritettäessä käytetään alajärjestelmää vastaavan komponentin valmistajan antamia arvoja $MTTF_d$-tason määrittämiseksi. Riippuen valitusta luokasta, näkyviin tulee myös DC_{avg}- ja CCF-välilehdet. Keskimääräinen diagnostiikan kattavuus voidaan määrittää lohkoista tai se voidaan syöttää suoraan. Standardissa ISO 13849-1 (2008) taulukossa E.1 on esitetty esimerkkejä diagnostiikan kattavuudesta. Mikäli alajärjestelmä vaatii yhteisvikaantumisen estämiseksi tehtyjen toimenpiteiden tutkimista, voidaan ne määrittää CCF-välilehdellä. Toimenpiteet valitaan kirjastosta, jossa ne on esitetty standardin ISO 13849-1 (2008) taulukon F.1 mukaisesti.

4.4 Lohko

Lohkoja luodaan alajärjestelmän kanaviin/kanavaan (riippuen alajärjestelmän luokasta) joko tekemällä kokonaan uusi lohko tai jälleen käyttämällä valmistajan lohkoksi luokiteltua valmista komponenttia. Tällainen komponentti voi olla esimerkiksi lukko, jossa on useita kytkimiä sisällään.

Mikäli luodaan kokonaan uusi lohko, voidaan sen Dokumentaatio-välilehdellä määrittää lohkolle nimi sekä kertoa lisää tietoa lohkosta. $MTTF_d$-välilehdellä voidaan lohkolle määrittää suoraan vaarallinen keskimääräinen vikaantumisaika (tällöin lohkoon ei voi lisätä elementtejä) tai se voidaan laskea lohkoon kuuluvista elementeistä.

4.5 Elementti

Elementti on koko turvajärjestelmän pienin osa. Se voi olla esimerkiksi jonkin lohkon mekaaninen osa. Elementti voidaan hakea valmistajan kirjastosta tai sellainen voidaan luoda. Elementti nimetään ja sille annetaan jokin seuraavista alasvetovalikosta valittavista tyypeistä: sähkömekaaninen (esim. kela), elektroninen (esim. diodi), hydraulinen (esim.

sylinteri), mekaaninen (esim. rajakytkimen vipuvarsi), pneumaattinen (esim. paineilmakytkimen pneumaattinen osa) tai jokin muu komponentin tyyppi, joka ei sovi mihinkään edellä mainituista kuvauksista.

Jokaiselle elementille voidaan määrittää diagnostiikan kattavuuden taso DC-välilehdeltä. Elementtien diagnostiikan kattavuus vaikuttaa koko järjestelmän keskimääräiseen diagnostiikan kattavuuteen. Elementin DC-arvo voidaan syöttää suoraan, jolloin se tulee perustella Dokumentaato/johtopäätökset -kentässä. Vaihtoehtoisesti diagnostiikan kattavuus voidaan määrittää kirjastosta, jonne on koottu standardissa ISO 13849-1 (2008) taulukossa E.1 esitettyjä DC-tason määrittämiseen sovellettavia toimenpiteitä. Näistä valitaan sopiva toimenpide, joka määrää elementin DC-tason ja antaa toimenpiteelle automaattisesti kuvauksen.

4.6 Projektin mallintaminen SISTEMA:ssa

Jotta projektiin liittyviä turvatoimintoja (sähköisiä/mekaanisia kytkentöjä) voitaisiin mallintaa SISTEMA:ssa, on helpointa luoda suunnitellusta kytkentäkaaviosta lohkokaaviomallinnus. Kytkennän mallintamista SISTEMA:aan on esitetty tarkkaa opastusta IFA:n luomassa SISTEMA Cookbook 1:ssä. IFA on luonut myös useita muita Cookbook -oppaita, joissa kerrotaan lohkokaavioiden muodostamisesta erilaisista piireistä. Kaikki oppaat ovat ilmaisia ja ladattavissa IFA:n sivuilta. Sivuilta löytyy myös esimerkkejä erilaisten piirien SISTEMA-malleista.

4.6.1 Lohkokaavion luonti

Lohkokaavion luonti SISTEMA:aa varten tapahtuu helpoiten vaiheittain. Liitteessä 5 on esitetty lohkokaavion muodossa miten turvajärjestelmän muuntaminen lohkokaavioksi kulkee askeleittain alusta loppuun. Menetelmä koostuu kaikkiaan yhdeksästä eri vaiheesta, joista jotkut on jaettu osiin. Seuraavassa on käännetty ja lyhennetty englanninkielisestä Apfeld, Hauke, Rempel, ja Ostermanin (2010) SISTEMA Cookbook (versio 1.0) -oppaasta nämä edellä mainitut vaiheet.

Vaihe 1.

Ensimmäisen toiminnallisen kanavan komponenteista muodostetaan lohkoja (block) ja ne järjestetään vasemmalta oikealle. Vasemmanpuoleisimpina lohkoina ovat anturit, kytkimet yms. ja oikeanpuolimmaisena toimilaitteet.

Vaihe 2.

Jokainen yksittäinen lohko ensimmäisessä tulokanavassa sisällytetään alajärjestelmään, joka luokitellaan sen ominaisuuksien perusteella johonkin kappaleessa 3.4 esitettyyn luokkaan.

Vaihe 3.

Mikäli valmistaja on antanut komponentille valmiiksi PL- tai PFH-arvon, voidaan komponentti tulkita kapseloiduksi alajärjestelmäksi. Tällöin komponentin sisäistä rakennetta (lohkoja ja elementtejä) ei tarvitse tarkastella pidemmälle.

Vaihe 4.

Seuraavaksi tarkastellaan komponentin vian paljastumista. Vikaantumismalleja on lueteltuna standardissa SFS-EN ISO 13849-2. Jokaisessa vikaantumisessa tulee tarkastella onko vika vaaraton vai vaarallinen turvajärjestelmän toiminnan kannalta. Jos komponentin kaikki viat voidaan sulkea pois, lohkoa voidaan käsitellä kapseloituna alajärjestelmänä, jolloin se ei vaadi tämän aiheen osalta pidempää tarkastelua.

Vaihe 5.

Mikäli komponenteissa on mahdollista esiintyä vikoja, tarkastellaan seuraavaksi aiheuttaako vian ilmaantuminen turvatoiminnon menetyksen. Jos aiheuttaa, siirrytään kaaviossa kohtaan kuusi. Muutoin jatketaan kohdasta 5a.

Vaihe 5a

Jos turvatoiminto säilyy yhden tai useamman rinnakkaisen komponentin toimesta, kun tarkasteltavana oleva lohko vikaantuu, nämä rinnakkaiset lohkot esitetään toisessa toiminnallisessa kanavassa. Mikäli rinnakkaisia komponentteja on lisätty, täyttyvät luokkien 3 ja 4 mukaiset ehdot eikä näin ollen yksittäisen vian esiintyminen yhdessä komponentissa toisessa kanavista johda turvatoiminnon menettämiseen. Tämän lisäksi luokan kolme vaatimuksiin kuuluu myös, että komponenttien yksittäiset viat havaitaan, mikäli se on järkevällä tavalla mahdollista.

Vaihe 5b

Mikäli vaihe 5a täyttyy, tutkitaan seuraavaksi kumpi luokista 3 ja 4 täyttyy. Luokan 4 ehtojen täyttymiseksi, ei alajärjestelmän kahden vian huomaamatta jääminen saa johtaa turvatoiminnon menetykseen. Mikäli toisen vian huomaamatta jääminen johtaa turvatoiminnon menettämiseen, kuuluu alajärjestelmä luokkaan 3. Katso myös muut luokkien täyttymiseen liittyvät ehdot kappaleesta 3.4.

Vaihe 6

Jos alajärjestelmä ei ole täyttänyt mitään vaiheessa viisi esitettyjä ehtoja, se ei kuulu luokkiin 3 tai 4. Mikäli kuitenkin lohkon vika havaitaan testikanavan toimesta ja tämän toimesta turvallinen tila saadaan aikaan, täyttyvät luokan 2 mukaiset ehdot.

Vaihe 6b

Luokkaan 2 kuuluvaan alajärjestelmään lisätään testikanava, johon liitetään vikaa tutkivat lohkot. Tällöin turvatoimintoa täytyy testata sopivan aikavälein. Kun näin menetellään, turvatoiminnon menetys havaitaan ja turvallinen tila saavutetaan erillisellä erotuslaitteella. Erotuslaitetta ohjaa testauskanavan lohko/lohkot.

Vaihe 7

Mikäli alajärjestelmä ei sisällä minkäänlaista testausta tai rinnakkaisuutta, voidaan sillä päästä ainoastaan luokkiin 1 ja B. Luokkaan 1 vaaditaan, että käytetty komponentti on hyvin koeteltu (ks. SFS-EN ISO 13849-1 2008). Jos komponentin ei voida todeta olevan hyvin koeteltu, päädytään alajärjestelmän osalta luokkaan B.

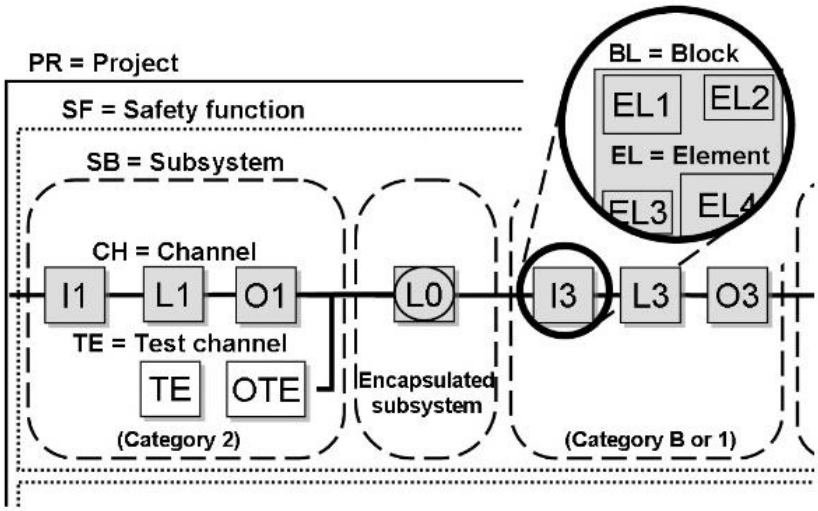
Vaihe 8

Mikäli kaikkia lohkoja ei ole analysoitu palataan vaiheeseen kaksi, muutoin jatketaan vaiheeseen yhdeksän.

Vaihe 9

Lopuksi kaikki samaan luokkaan kuuluvat alajärjestelmät yhdistetään yhdistämällä samanlaisten kanavien komponentit. Näin jokainen komponentti esiintyy vain kerran kanavassa ja samanlaiset komponentit tulee poistaa. Samaa komponenttia ei voi myöskään käyttää saman alajärjestelmän molemmissa rinnakkaisissa kanavissa. Luokkaan 2 kuuluvien alajärjestelmien komponentit, jotka jakavat saman testikanavan, voidaan yhdistää samaksi kanavaksi. Yhdistämällä samanlaiset komponentit saavutetaan korkeampi $MTTF_d$-arvo (tästä seuraa korkeampi PL-taso).

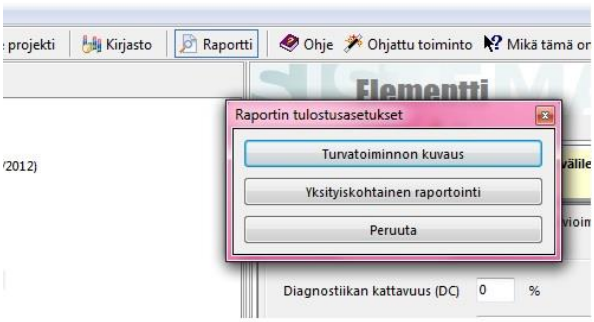
Lohkokaavion muodostaminen vaatii turvajärjestelmän sisäistämistä ja piirikaavion saattaminen SISTEMA:lle ymmärrettävään muotoon on aloittelevalle käyttäjälle vaativa toimenpide. Kuvassa 3 on esitetty miten SISTEMA:n eri hierarkian tasot esiintyvät lohkokaaviossa. Piirikaavioiden kääntämisessä SISTEMA:n lohkokaavioiksi saattaa esiintyä käyttäjien välillä myös tulkinnallisia eroja.



KUVA 3. Lohkokaavion hierarkiatasot SISTEMA:ssa (Apfled ym. 2010, 15)

4.7 SISTEMA raportti

Kun turvajärjestelmä on luotu SISTEMA:n avulla, siitä voidaan tulostaa loppuraportti. Loppuraportti tulostetaan SISTEMA-ikkunan ylälaidassa sijaitsevasta Raportti-painikkeesta (ks. kuva 4). Painikkeesta avautuu ikkuna, jossa valitaan raportin tulostusasetukset. Turvajärjestelmästä voidaan tulostaa pelkkä turvatoiminnon kuvaus, joka sisältää projektin kuvauksen ja siihen liittyvät standardit. Tässä raportissa ilmenee myös projektiin liittyvät turvatoiminnot (SF) sekä niille määritetyt vaadittavat suoritustasot ja suoritustasot, johon turvatoiminolla päästiin. Turvatoiminnon kuvaus -raportti on lyhyempi (n. 2 sivua riippuen turvatoimintojen määrästä) kuvaus projektin turvatoiminnoista.



KUVA 4. Raportin tulostus

Mikäli projektista halutaan tulostaa pidempi, kaiken kattava kuvaus, valitaan raportin tulostusasetukset -ikkunassa "yksityiskohtainen raportointi". Yksityiskohtaisessa raportoinnissa ilmenee seuraavat asiat:

- projektin nimi ja kuvaus sekä käytetyt standardit

- jokainen projektin turvatoiminto ja niiden yksityiskohtainen kuvaus mm. PLr-tason määritys riskigraafista sekä saavutettu PL-taso
- kaikki turvatoimintojen alla olevat alajärjestelmät ja niiden suoritustasot yms.
- alajärjestelmien kanavat sekä niissä olevat lohkot
- lohkoihin kuuluvat elementit ja niiden tyypit, kuvaukset yms.

Turvajärjestelmän yksityiskohtainen raportti on siis laajuudeltaan huomattavasti kattavampi kokonaisuus.

5 CM4 LAMINAATTORIN TURVA-ALUE

UPM Raflatac Oy:n Tesoman tehtaalla on suunniteltu ja toteutettu turva-alueita joidenkin koneiden alueille. Kyseiset alueet ovat turvahäkin sisässä olevia koneen osa-alueita, joiden on katsottu tarvitsevan turvallisuuden takaamiseksi ympärilleen metallisen suojahäkin. Häkki koostuu aidoista sekä yhdestä tai useammasta ovesta, joista häkkiin päästään sisälle esimerkiksi telojen puhdistamista varten. Ovissa on turvalukot, jotka avataan painonapeilla. Oven avaaminen käynnistää alueen turvatoiminnon/-toiminnot.

Myöhemmin esiteltävässä CM1 kiinnirullaimen turva-alueen suunnittelussa on käytetty pohjana tässä kappaleessa esiteltävää CM4 laminaattorin turva-alueen kytkentää ja toteutusta. Tämän vuoksi tein CM4 laminaattorin turva-alueesta SISTEMA-ohjelmistolla mallinnuksen nykyisen turva-alueen PL-tasosta sekä kehitin mallin pohjalta parannusehdotuksen kytkennästä ja mallinsin vielä sen SISTEMA:lla.

5.1 Nykyisen turva-alueen kytkentä

Nykyisen laminaattorin turva-alueen piirikaavio on esitetty liitteessä 6. Kytkennän tarkoituksena on katkaista ylä-, ala- ja imutelan moottoreilta sähköt sekä katkaista paineilman syöttö pneumaattisilta laitteilta, kun turvaovi avataan ja alueella oleskelee henkilöitä. Näin estetään mahdollinen telojen ja pneumaattisten laitteiden vahinkokäynnistyminen, jolloin alueella työskentely on turvallista.

Turvatoimintoja ohjaa Phoenix PSR 300 –turvarele (liitteessä 6 R-9016.1). Turvarele valvoo siihen liitettyjen kahden oven *”kiinni”*- ja *”lukossa”*-tietoja. Kuvaan on jätetty myös varaus mahdollisesti lisättävälle ovelle ja sen lukitustiedoille. Lukkona on käytetty Bernsteinin SLK-sarjan turvalukkoa. Lukosta saadaan avautuvilla koskettimilla *"kiinni"*- ja *"lukossa"*-tiedot. Oven avaaminen tapahtuu kunkin oven sivussa olevasta avauspainikkeesta. Tätä ennen vaaditaan kuitenkin järjestelmästä avauslupa (liitteessä 6 R-9016.3). Avauslupa tulee, kun koneet ovat pysähdyksissä.

Painettaessa kumman tahansa oven avauspainiketta, lakkaa turvarele R-9016.1 vetämästä. Tällöin telojen moottorien kontaktoreja ohjaavat Pilz:n PZE X4 turvareleet mene-

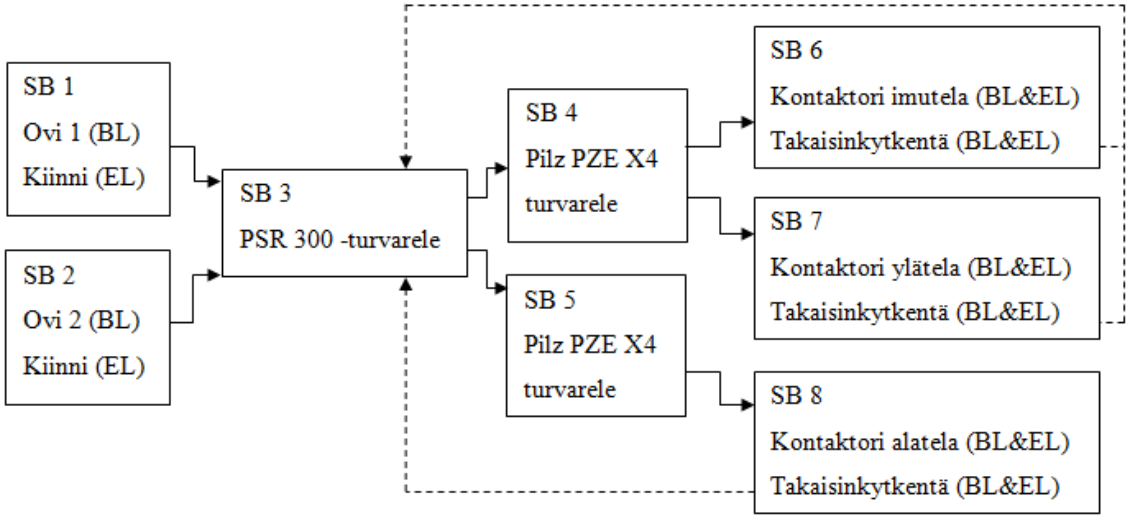
vät energiattomaksi, jolloin moottorien käynnistyminen ei ole mahdollista. Moottorikontaktorien tilan vaihtumista valvotaan avautuvien koskettimien takaisinkytkennällä kontaktoreilta turvareleelle R-9016.1. Tällä varmistutaan siitä, että kontaktorit ovat toimineet ja energia moottoreilta poistunut. Myös pneumatiikkakotelolta katkaistaan ilmansyöttö venttiilin EGV-9016.1 mennessä energiattomaksi.

Ovien avautumista ohjaavat turvareleen koskettimet 67 ja 68 ovat päästöhidasteisia. Tällä saadaan asetettua varmistusaika telojen täydelliselle pysähtymiselle. Ovien avautumista ohjaava rele R-9016.2 ei lakkaa vetämästä ennen kuin säädetty aika oven avauspainikkeen ja turvareleen R-9016.1 laukeamisesta on kulunut. Kun asetettu aika on kulunut ja rele R-9016.2 lakkaa vetämästä, sulkeutuu sen avautuva kosketin ja lukkojen solenoidit saavat sähkön avauspainikkeen ollessa pohjassa. Tällaisella kytkennällä saadaan luotua turvallinen energiaton työskentely alue. Turvareleen R-9016.1 laukeamisen jälkeen se täytyy kuitata oven vieressä olevasta kuittauspainikkeesta. Kuittaantuminen vaatii kuitenkin, että molemmat ovet ovat kiinni ja lukossa.

5.2 Turva-alueen SISTEMA-malli

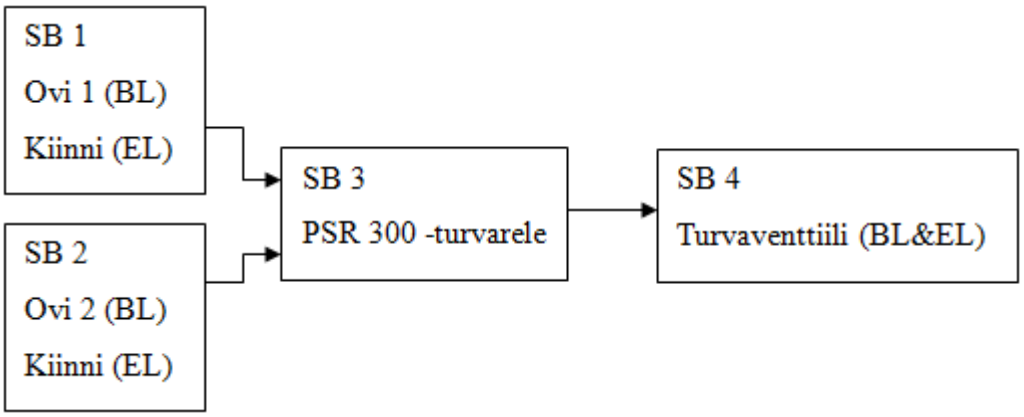
Jotta edellä mainittua kytkentää voitaisiin mallintaa SISTEMA-ohjelmistolla ja laskea sille PL-taso, tulee kytkentäkaaviosta muodostaa kappaleessa 4.6.1 käsitelty lohkokaavio. Helpoin tapa alkaa muodostamaan lohkokaaviota on miettiä mitä turvatoimintoja (SF) kytkentään sisältyy. Tässä tapauksessa voidaan ajatella turvatoimintoja olevan kaksi kappaletta: moottorien käynnistyksen esto (kaikki kolme kuuluvat samaan turvatoimintoon) ja paineilmojen poisto. Seuraavaksi kannattaa pelkistää turva-alueen kytkentäkaavio (ajatuksellisesti) ja miettiä mitkä ovat turvatoimintoon liittyviä komponentteja. Tässä tapauksessa turvatoimintoon kuuluvia elementtejä ovat tulopuolella ovien *”kiinni”*-tiedot. Turvallisuuden kannalta oleellista on tieto siitä, että ovi on kiinni, ei niinkään onko se lukossa vai ei. Toimintojen suorittamisesta vastaa turvarele R-9016.1 eli se on oleellinen osa turvatoimintoa. Lähtöpuolella oleellisia komponentteja ovat Pilz:n PZE X4 turvareleet sekä moottorien kontaktorit ja niiden takaisinkytkentätiedot. Myös paineilmaventtiili kuuluu lähdöiksi luokiteltaviin komponentteihin. Itse ovien avaamiseen liittyvät komponentit kuten rele R-9016.2 ja oven avauspainikkeet eivät ole osana mitään turvatoimintoa, sillä ne eivät toteuta mitään turvallisuuteen liittyvää toimintoa.

Kun kytkentäkaavio on ajatuksellisesti saatu pelkistettyä ja turvatoimintoihin liittyvät komponentit ovat selvillä, voidaan seuraavaksi alkaa luomaan kytkentäkaaviosta lohkokaaviota. Ensiksi tarvitsee luokitella komponentit alajärjestelmiin (SB) ja miettiä mihinkä luokkaan (ks. kappale 3.4) alajärjestelmä kuuluu. Tämän jälkeen muodostetaan lohkot (BL) ja niiden elementit (EL). Standardin SFS 13849-1 mukaan sama komponentti voi olla mukana toteuttamassa yhtä tai useampaa turvatoimintoa, joten tässä tapauksessa ovien *"kiinni"*-tietoja käytetään molemmissa turvatoiminnoissa tulopuolella. Kuviossa 6 on esitetty käynnistyksenesto-turvatoimintoa kuvaava lohkokaavio. Kuviossa katkoviivalla on esitetty kontaktorien takaisinkytkentätieto logiikalla. Turvareleet PSR 300 sekä molemmat Pilz PZE X4:t ovat kokonaisia, valmistajan määrittämiä alajärjestelmiä.



KUVIO 6. Käynnistyksenesto-turvatoiminnon lohkokaavio

Vastaavasti paineilman poisto-turvatoiminnosta on alla esitetty lohkokaavio (kuvio 7), jossa tuloina ovat myös ovien *"kiinni"*-tiedot ja toiminnon suorittajana PSR 300 -turvarele. Lähtönä tässä toiminnossa on magneettiventtiili EGV-9016.1. Venttiililtä ei ole minkäänlaista takaisinkytkentää.

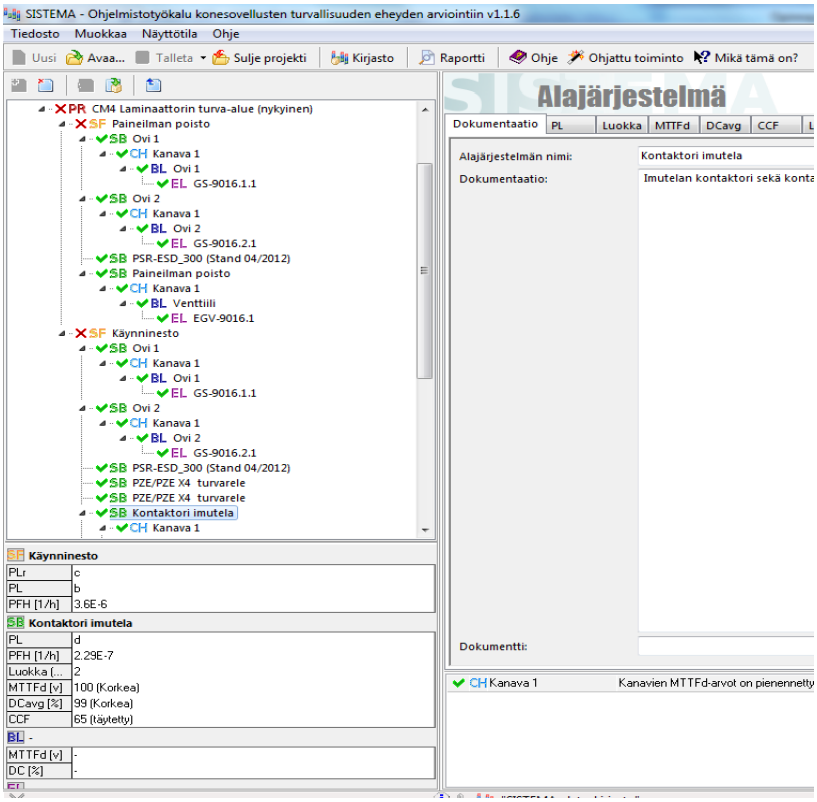


KUVIO 7. Paineilmojen poisto -turvatoiminnon lohkokaavio

Kun lohkokaaviot on luotu, voidaan turvatoiminnot muodostaa SISTEMA-ohjelmistolla. Ensimmäisenä luodaan uusi projekti ja sille turvatoiminnot. Turvatoimintojen alle lähdetään tekemään alajärjestelmiä. Mikäli komponentin valmistajalta löytyy SISTEMA-kirjasto ja sieltä valmistajan määrittämät tiedot komponentille, tulisi käyttää niitä yleisten asetusten sijaan. Ovien lukkojen koskettimille ei löydy suoraan valmistajan määrittämää komponenttia, joten ne luodaan manuaalisesti. Kosketinelementeille valitaan sopiva B_{10d}-arvo kirjastosta. Tässä tapauksessa ovien standardin mukainen luokka on 1, sillä tulo on yksikanavainen ilman minkäänlaista diagnostikkaa. Phoenixin PSR 300 -turvareleelle löytyy valmistajalta SISTEMA-kirjasto (ladattava erikseen), josta löytyy kyseinen komponentti ja sille luokka (luokka 4) sekä suoritustaso PL e. Samoin löytyy myös Pilz:n PZE X4 releelle. Valmistaja antaa luokaksi 4 ja PL-tasoksi PL e. Koska releeltä ei ole tässä kytkennässä tuotu valmistajan vaatimaa takaisinkytkentää, pudotin sen luokan luokkaan 3 ja PL-tason PL d:ksi.

Moottorien kontaktorit ovat myös omia alajärjestelmiään. Koska niiltä on takaisinkytkentä PSR 300 -turvareleelle, voidaan kontaktorien alajärjestelmän luokaksi asettaa luokka 2. Sen sijaan paineiden poistoventtiililtä ei ole minkäänlaista takaisinkytkentätietoa, joten se voidaan perustellusti asettaa enimmillään luokkaan 1. $MTTF_d$-arvojen määrittämisessä komponenteille, joille ei ole valmistajan kirjastoa, on käytetty yleisimpiä komponenttien $B10_d$-arvoja ja toimintajaksoina/vuosi arvoa 3600 (300 päivää, 24 h/päivä, 7200 s/sykli) (ks. kappale 3.2).

Kun vaadittavat arvot on määritelty, näkyy SISTEMA:ssa kuvan 5 mukainen hierarkia. Kutakin hierarkian tasoa klikkaamalla voidaan nähdä siihen liittyvät arvot sekä turvatoiminnon suoritustaso PL.



KUVA 5. Esimerkki SITEMA-projektin hierarkiasta

Laminaattorin turva-alueen vaadittavaksi suoritustasoksi on määritelty PL_r c, joten molempien turvatoimintojen tuli yltää tälle suoritustasolle. Nykyisellään molemmat turvatoiminnot yltävät ainoastaan suoritustasolle b. Tämän vuoksi kuvassa 5 olevien projektin (PR) sekä turvatoimintojen (SF) edessä näkyy punainen ruksi. Seuraavassa kappaleessa on esitelty paranneltu malli ja kytkentäkaavio, jolla päästään vaadittuun suoritustasoon.

5.3 Turva-alueen paranneltu malli

Turvallisuutta saadaan parannettua usein tekemällä vain pieniä lisäyksiä, jotka eivät kustannuksiltaan ole välttämättä kovinkaan suuria. Edellä käsitellyn laminaattorin turva-alueen suoritustason parantamiseksi tarvitaan vain muutama rajakytkin sekä pieni kytkentämuutos. Liitteessä 7 on esitetty paranneltu kytkentäkaavio, jolla päästään paineilman poiston osalta suoritustasoon PL d ja käynnineston osalta suoritustasoon PL c. Käynnineston suoritustaso putoaa PL c suoritustasoon, sillä järjestelmä sisältää enemmän kuin kolme PL d tason alajärjestelmää (ks. taulukko 4). Kytkentäkaaviossa turvareleen toiseen tulokanavaan on liitetty nyt molempiin oviin lisätyt magneettiset rajakytkimet ja niiden

avautuvat koskettimet. Magneettisina rajakytkiminä käytetään tässä tapauksessa Mechanin MS6-sarjan rajakytkimiä (kuva 6).

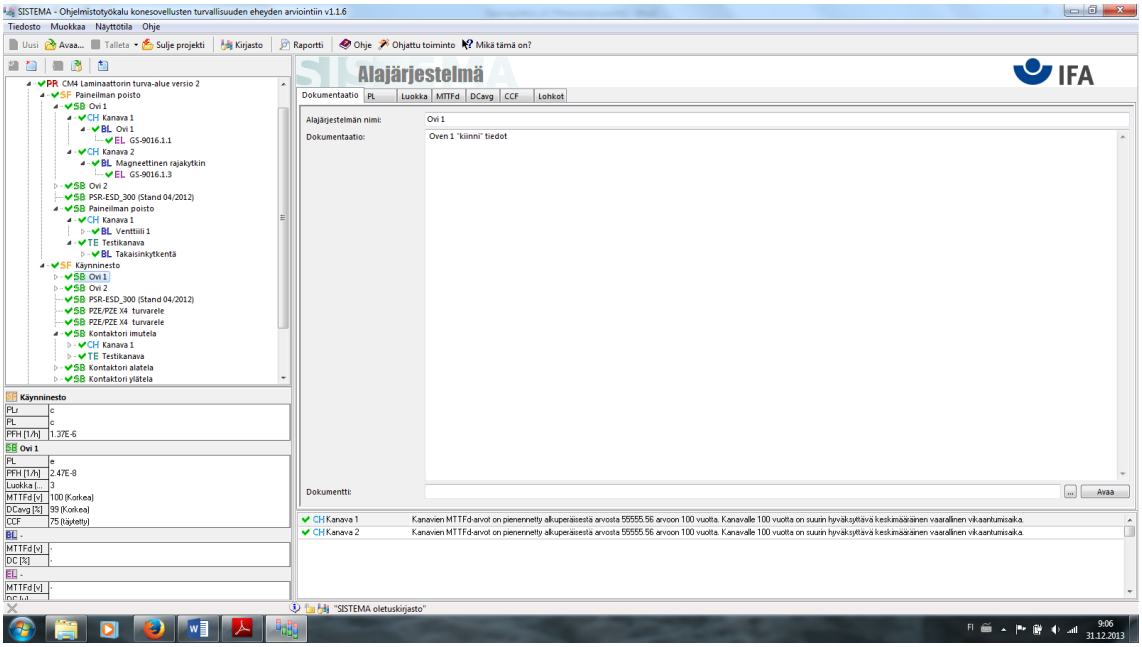
KUVA 6. Mechan MS6-sarjan magneettisia rajakytkimiä (OEM Finland Oy 2014)

Nyt turvareleelle saadaan kahdennettu tulo ovien *”kiinni”*-tilasta, jolloin tulopuolen alajärjestelmät kuuluvat luokkaan 3. Lähtöpuolella, käynnistykseneston osalta, takaisinkytkentäsilmukkaan on lisätty Pilz:n turvareleiden takaisinkytkentätieto, jolloin niiden suoritustaso voidaan nostaa valmistajan määrittämälle tasolle PL e. Nyt siis valvotaan myös, että moottorikontaktoreita ohjaavat turvareleet ovat toimineet. Paineilman poistoon on lisätty myös valvontaa. Aiemmassa kytkennässä ei voitu olla varmoja ovatko paineilmat poistuneet. Nyt tämä asia on korjattu lisäämällä paineilmalinjaan Suco:n painekytkin (kuva 7), jolla valvotaan magneettiventtiilin toimintaa.

KUVA 7. Suco painekytkin (OEM Finland Oy 2014)

Näin saadaan arviolta muutaman sadan euron kustannuksilla paranneltua kytkentää siten, että saavutetaan vaadittu suoritustaso ja turvattavasta alueesta saadaan turvallisempi.

Muunneltu kytkentä mallinnetaan uudestaan SISTEMA-ohjelmistolla. Edelliseen versioon tarvitsee tehdä vain muutama muutos mm. ovien luokan vaihto luokasta 1 luokkaan 3. Kuvassa 8 näkyy SISTEMA-näkymä päivitysten jälkeen. Nyt molempien turvatoimintojen sekä projektin tila on vihreä, koska ne täyttävät asetetun vaaditun suoritustason.



KUVA 8. SISTEMA-näkymä päivitysten jälkeen

6 TURVAJÄRJESTELMÄN KOMPONENTTIEN VALINTA

Standardissa SFS 13849-1 (2008) sanotaan, että luokkaan 1 ja sitä ylempiin luokkiin kuuluvissa järjestelmissä tulisi käyttää hyvin koeteltuja komponentteja. Hyvin koetelluiksi komponenteiksi voidaan tulkita esimerkiksi sellaiset komponentit, joille valmistaja on määrittänyt turvallisuuteen liittyviä arvoja. Nämä komponentit ovat valmistajan toimesta testattuja ja niille on määritetty mm. B_{10d}-arvo, PL-taso tai SIL-luokka. Näitä arvoja tulee käyttää myös laskettaessa suoritustasoa turvallisuuteen liittyvälle ohjausjärjestelmälle. Turvallisuuden kehittyessä jatkuvasti ja sen merkityksen kasvaessa, on aloitettu valmistamaan turvakomponentteja. Jälleenmyyjien sivustoilla turvakomponentit erotetaan usein normaaleista komponenteista asettamalla ne omaan alahakemistoonsa. Myös komponenttien nimen eteen on laitettu sana ”turva” esimerkiksi turvarajakytkimet.

Näillä turvajärjestelmiin tarkoitetuilla komponenteilla on usein saksalaisen TÜV:n (saks. Technischer Überwachungsverein) tarkastuslaitoksen myöntämä sertifikaatti. Sertifikaatilla todennetaan asiakkaalle, että komponenttia on testattu ja sille on saatu määritettyä turvallisuuteen liittyviä arvoja. Liitteessä 8 on esimerkki sertifikaatista paineilman poistossa käytetylle Numatics:n venttiilille. Turvallisuuteen liittyvän järjestelmän ei kuitenkaan tarvitse koostua turvakomponenteista, vaan siinä voidaan käyttää myös tavallisia komponentteja. Tavallisilla komponenteilla on usein vain huonommat turvallisuusarvot ja tämän vuoksi ne saattavat laskea koko järjestelmän suoritustasoa.

Raflatac Oy:n Tampereen tehtaalla on useimmissa turvallisuuteen liittyvissä järjestelmissä päädytty ohjauksen osalta turvareleisiin logiikan sijaan. Releiden käyttö on huomattavasti helpompaa, sillä turvalogiikkaa käytettäessä täytyy tarkastella myös ohjelman suoritustasoa ja sen toiminnan varmuutta omana kokonaisuutenaan. Lisäksi turvalogiikan käyttö lisää virheiden mahdollisuuksia ohjauksissa juuri ohjelman takia. Tehtaalla tuloja ja lähtöjä prosessoivaksi turvareleeksi on kokemusten myötä valikoitunut Phoenix PSR 300 –turvarele (kuva 9). Tässä turvareleessä on sopiva määrä sulkeutuvia koskettimia lähtöjen ohjaamiseksi, kaksi- tai yksikanavaisen tulon mahdollisuus sekä päästöhidastus. Rele sopii useimpiin käyttökohteisiin koko tehtaalla ja siksi se on valittu käytettäväksi myös myöhemmin esiteltävässä CM1 kiinnirullaimen turva-alueessa.

KUVA 9. Phoenix PSR 300 -turvarele (Phoenix Contact Oy 2014)

Kun halutaan ohjata moottorien kontaktoreita, on PSR 300 –turvareleen ja moottorin kontaktorin väliin laitettu laajennusyksikkö Pilz:ltä (kuva 10). Pilz PZE X4 on myös turvarele, mutta vähemmillä ominaisuuksilla kuin PSR 300. Releessä on kahdennettu kela ja koskettimet, mikä tekee siitä turvallisemman komponentin verrattuna tavalliseen releeseen. PZE X4:ssä ei kuitenkaan ole vastaavaa älykkyyttä kuin PSR 300:ssa ja sitä käytetäänkin vain tavallisen releen tapaan. Releestä saatava takaisinkytkentä valvoo molempien kelojen toimintaa.

KUVA 10. Pilz PZE X4 –turvarele (Pilz GmbH & Co. KG 2014)

Kuten aiemmin käsitellyn CM4 laminaattorin turva-alueessa, myös tulevassa CM1:n kiinnirullaimen turva-alueessa tarvitaan paineilmojen katkaisu –toimintoa alueen turvallisuuden takaamiseksi. Laminaattorin turva-alueella käytetty ASCO 327-sarjan 3/2 magneettiventtiili (kuva 11) valittiin myös CM1:lle paineilmojen katkaisuun pneumatiikkakotelolta. Paineilmojen poistumista valvotaan aiemmassa kappaleessa kuvassa 7 esitetyllä Suco:n painekytkimellä.

KUVA 11. ASCO 327-sarjan magneettiventtiili (SITEK-PALVELU OY 2014)

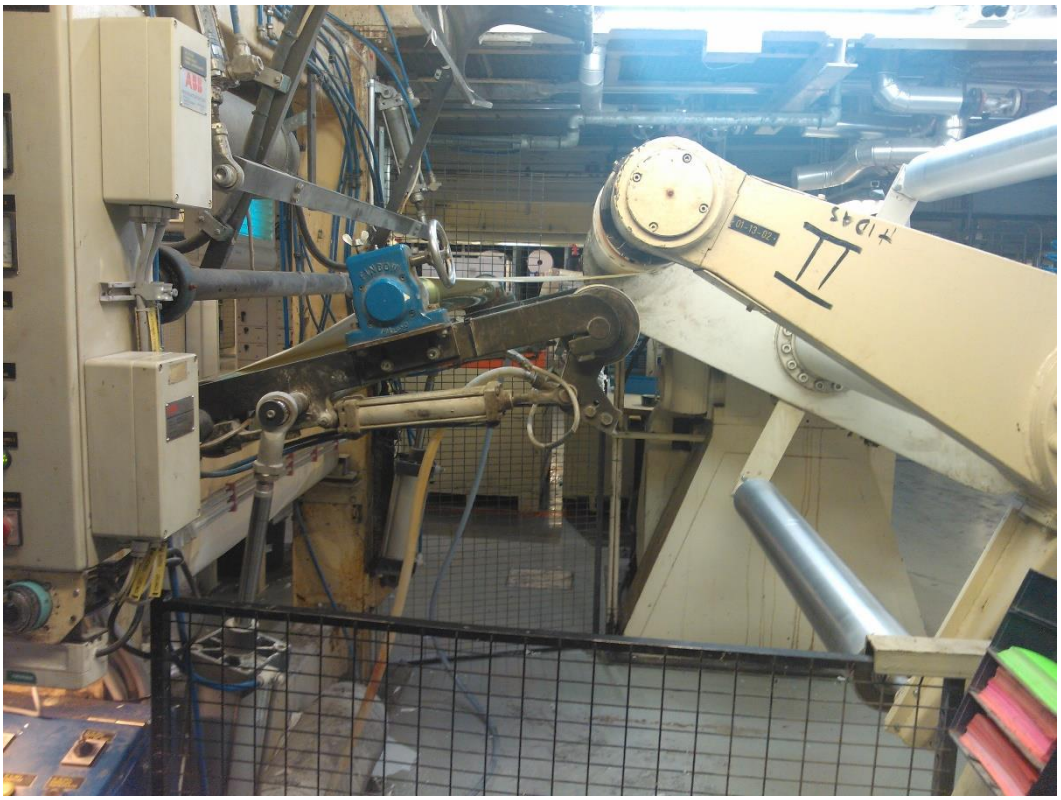
CM1:n kiinnirullaimella tarvitaan myös hydrauliikan kierron sulku sekä hydrauliikan pysäytys. Kierron sulku toteutetaan hydrauliikkaventtiileillä, jotka toimittaa hydrauliikkakoneikon asentaja. Karusellin kääntömoottoria, kara-akselien käyttöjä sekä hydrauliikkapumppua ohjataan tavallisilla kontaktoreilla ja kontaktoreita ohjataan aiemmin esitetyillä Pilz:n turvareleillä. Kiinnirullaimelle tulee vain yksi ovi, jolla hallitaan alueelle pääsyä. Oven tarvikkeet (lukko, ovi yms.) tilataan OEM AUTOMATIC:lta (OEM Finland Oy), samoin kuin magneettiset turvarajakytkimet ja painekytkin.

Kiinnirullaimen poisottoalue on turvattu SICK:n valmistamilla M 4000 sarjan valoverholla (kuvassa 12 vasemmalla). Valoverhojen toimintaa valvoo UE 10-3 OS valoverhorele (kuvassa 12 oikealla). Valoverhojen rikkoutuessa rele lakkaa vetämästä, jolloin kosketin aukeaa. Valoverhoreleen aktivoiminen tarvitsee erikseen kuittauksen.

KUVA 12. SICK valoverho ja valoverhorele (SICK AG 2014)

7 CM1 KIINNIRULLAIMEN TURVAJÄRJESTELMÄN TOTEUTUS

CM1 on yksi vanhimpia laminointikoneita tehtaalla ja sen turvallisuudessa on paljon päivitettävää nykypäivän vaatimusten tasolle. Työni aiheessa keskitytään kuitenkin yhden osa-alueen eli kiinnirullaimen turva-alueen päivitykseen. Kiinnirullaimen turva-alue koostuu käytännössä kahdesta osasta: vaihtoalueesta ja poisottoalueesta. Vaihtoalue (kuva 13) on karusellin takapuolella oleva alue, jossa rulla liittyy rataan. Vaihtoalue suojataan kokonaisuudessaan häkillä ja alueelle pääsy ajon aikana ei ole mahdollista. Tämä voidaan ja täytyy toteuttaa näin, sillä alueella oleskelu ei ole tarpeen ajon aikana. Alueella on useita vaaratekijöitä, kuten puristuminen johtuen karusellin aiheuttamasta liikkeestä tai vahingoittuminen radankatkaisuterän liikkeestä. Nykyinen n. 1 metrin korkuinen aita ei suojaa mitään ajon aikana tapahtuvaa kulkua alueelle, sillä aita on myös avattavissa ilman minkäänlaista pysäytysreaktiota.



KUVA 13. Kiinnirullaimen vaihtoalue nykyisellään

Poisottoalue (kuva 14) on vastaavasti karusellin etupuolella sijaitseva alue, jossa tapahtuu täyden rullan poisottaminen karusellista ja uuden hylsyn laitto uutta rullaa varten. Alueen turvaamista hankaloittaakin juuri tarve käsitellä alueella isoja rullia. Tämän

vuoksi aluetta on mahdoton laittaa kokonaisuudessaan häkin sisään. Ratkaisuksi on päätetty tehdä niin, että häkkiä tuodaan hieman karusellin ohitse, mutta poisottoalue jää kuitenkin avoimeksi. Molemmin puolin karusellia asennetaan valoverhot siten, että ne tulevat häkkiä vasten ja niiden kiertäminen ei ole mahdollista. Valoverholla estetään karusellin kääntömoottorin sekä karamoottorien käynnistyminen rullan vaihdon aikana.

KUVA 14. Kiinnirullaimen poisottoalue nykyisellään

7.1 Turva-alueen piirikaavion suunnittelu

Kiinnirullaimen turva-alueen suunnittelussa käytin pohjana kappaleessa 5 esitetyn CM4 laminaattorin turva-alueen piirikaaviota, sillä se on todettu aiemmin toimivaksi kytkennäksi. Piirikaavio kiinnirullaimesta on esitetty liitteessä 9. Koska piirikaavio on yleinen tehtaalla käytetty pohja, siinä näkyy varaukset kolmen oven tulotietojen liittämiseksi turvareleelle. Kiinnirullaimelle tulee vain yksi turvaovi, joten tämän vuoksi kaaviossa näkyy hyppy muiden ovien *”kiinni”*- ja *”lukossa”*-tietojen kohdalla. Kuten CM4 laminaattorin turva-alueen päivitetyssä versiossa, ovelta tuodaan lukosta saatavilla avautuvilla koskettimilla turvareleelle oven *”kiinni”*- ja *”lukossa”*-tiedot tulokanavaan yksi. Oveen lisäksi kiinnitettävältä magneettiselta rajakytkimeltä tuodaan NO-koskettimelta oven *”kiinni”*-

tieto turvareleen tulokanavaan kaksi. Näin saadaan kahdennettua oven tulotiedot, jolloin tulokanavan osalta täytetään luokan 3 mukaiset vaatimukset.

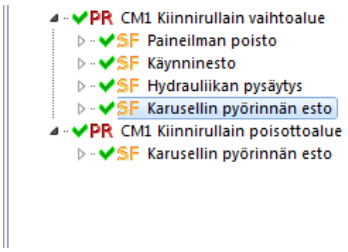
Turvareleellä ohjataan sulkeutuvien koskettimien kautta Pilz:n PZE X4 turvarelettä, joka vuorostaan ohjaa karamoottorien kontaktoreita. Karamoottorien kontaktorien avautuvat koskettimet ja Pilz turvareleen avautuva kosketin ovat osana PSR 300 -turvareleelle menevää takaisinkytkentälenkkiä. Toinen Pilz:n turvarele, joka ohjaa karusellin kääntömoottoria, puolestaan saa ohjauksen valoverhoreleen sulkeutuvan koskettimen kautta. Tällä estetään karusellin pyörintä. Myös karusellin kääntömoottoria ohjaavalta kontaktorilta sekä Pilz:n turvareleeltä on takaisinkytkentätieto avautuvien koskettimien kautta.

PSR 300:n toisella kosketinparilla ohjataan ASCO 327 –sarjan magneettiventtiiliä, joka poistaa paineilmat pneumatiikkakotelolta 113JK8. Paineilmojen poistumista valvotaan kappaleessa 6 esitetyllä painekytkimellä (osa takaisinkytkentälenkkiä). Toisella kosketinparilla ohjataan myös vaihtolaitteen hydrauliikkakoneikon kierron sulkuventtiilejä. Hydrauliikan kierron sulkeutumisesta ei ole takaisinkytkentätietoa. Hydrauliikkapumpun kontaktoria ohjaa myöskin Pilz:n turvarele. Turvarele puolestaan saa sähkönsä ensimmäisen PSR 300:n kosketinparin kautta. Hydrauliikkapumpun kontaktorilta ja turvareleeltä on takaisinkytkentätieto. Oven avauksen sallintareleen R-912.2 ohjaus tulee PSR 300 –turvareleen päästöhidasteisten koskettimien kautta. Päästöhidastuksella varmistetaan, että paineilmat ovat poistuneet ja koneet pysähtyneet. Ovien avaus toimii siis samoin kuin aiemmin esitetyssä CM4 laminaattorin turva-alueessa.

Kiinnirullaimella käytetään myös paineilmatyökalua, jonka käyttö on haluttu tehdä turvalliseksi. Tämä on toteutettu lisäämällä alueelle kaksi vahinkokäynnistyksenestokytkintä, jotka estävät kiinnirullaimen akselien 1 ja 2 käynnistymisen poisoton aikana. Kytkimet ovat kaksiasentoisia kytkimiä. Asennossa 1 akseleilla on mahdollisuus pyöriä ja asennossa 2 moottorien käynnistyminen on estetty. Paineilmatyökalu ei ole merkittävä osa koko kiinnirullaimen turva-alueella, joten sen mallintamista SISTEMA:lla ei ole toteutettu.

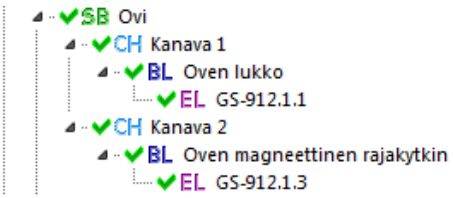
7.2 Kiinnirullaimen SISTEMA-mallinnus

SISTEMA:lla mallintamista ajatellen kiinnirullaimen turva-alue voidaan jakaa kahteen projektiin: vaihtoalueen turvatoiminnot ja poisottoalueen turvatoiminnot (kuva 15). Vaihtoalueen turvatoimintoja ovat paineilmojen poisto, karamoottorien käynninesto, hydrauliikan pysäytys sekä osittain myös karusellin pyörinnän esto. Poisottoalueella ainoa turvatoiminto on karusellin pyörinnän esto. Jokaisella edellä mainitulla toiminnolla päästään suoritustasolle PL d, mikä on edellytys rullaimilla. Jokainen turvatoiminto sisältää alajärjestelmänä oven ja PSR 300 -turvareleen. PSR 300 –turvareleen ja Pilz PZE X4 alajärjestelmien laskennassa on käytetty valmistajien SISTEMA-kirjastosta saatavia komponentteja.



KUVA 15. Kiinnirullaimen SISTEMA-projektit

Oven alajärjestelmän (Kuva 16) voidaan tulkita kuuluvaksi luokkaan 3, sillä kyseessä on kahdennettu tulo ja tulot ovat ristiinvalvottuja (tulojen yhtäaikainen toiminta) PSR 300 –turvareleen toimesta. Alajärjestelmässä kanavassa yksi on lukon *”kiinni”*-tieto ja toisessa kanavassa magneettiselta rajakytkimeltä saatava tieto.



KUVA 16. Oven alajärjestelmä SISTEMA:ssa

Turvaventtiilin alajärjestelmän (kuva 17) paineilman poisto -turvatoiminnossa voidaan ajatella kuuluvaksi luokkaan kaksi, sillä se on yksikanavainen lähtö (luokka kolme vaatisi kaksi sarjaan kytkettyä venttiiliä) ja sillä on valvonta painekytkimen kautta. Alajärjestelmän kanavaan yksi tulee venttiili, jolle on tässä tapauksessa valittu $B10_d$-arvo standardin

kirjastosta. Testikanavaan tulee painekytkimen elementti, jolle on myös valittu $B10_d$-arvo kirjastosta.

KUVA 17. Turvaventtiilin alajärjestelmä SISTEMA:ssa

Moottorien kontaktorien ohjaus voidaan myös ajatella kuuluvan luokkaa kaksi, koska niiden toimintaa valvotaan koskettimien takaisinkytkennällä. Koska kontaktoreita ohjaavat Pilz:n turvareleet ovat esitettävissä omina valmistajan määrittäminä alajärjestelminään, kuuluvat kontaktorien alajärjestelmiin vain kontaktori ja sen takaisinkytkentä. Kuvassa 18 on esitetty hydrauliikkapumpun kontaktorin alajärjestelmä, mutta myös kaikki muut kontaktorin ja Pilz:n turvareleen omaavat alajärjestelmät on toteutettu samoin.

KUVA 18. Hydrauliikkapumpun kontaktori -alajärjestelmä SISTEMA:ssa

Karusellin kääntömoottorin pyörinnän eston turvatoiminto (kuva 19) koostuu ovesta, PSR 300 –turvareleestä, Pilz:n turvareleestä, valoverhon turvareleestä, valoverhosta ja kääntömoottorin kontaktorista. Kaikki releet sekä valoverho ovat omia alajärjestelmiään ja niille löytyy valmiit valmistajan määrittämät SISTEMA-alajärjestelmät. Oven ja kääntömoottorin kontaktorin alajärjestelmät on luotu, kuten edellä on esitetty.

KUVA 19. Karusellin pyörinnän eston turvatoiminto

8 CM1 KIINNIRULLAIMEN TURVAJÄRJESTELMÄN KÄYTTÖÖNOTTO JA LOPPUDOKUMENTOINTI

Kiinnirullaimen turva-alueen päivitys sekä alueeseen liittyvät muut huoltotoimenpiteet toteutettiin seisakin aikana tammikuussa 2014. Asennukset valmistuivat ajallaan, jolloin myös alueen testaus päästiin aloittamaan ajoissa. Turvatoiminnot on tässä opinnäytetyössä eritelty aiemmin ja niistä on luotu oma ”Turvatoimintojen toiminnallinen kuvaus” –dokumentti Raflatac Oy:n käyttöön.

8.1 Turva-alueen testaus

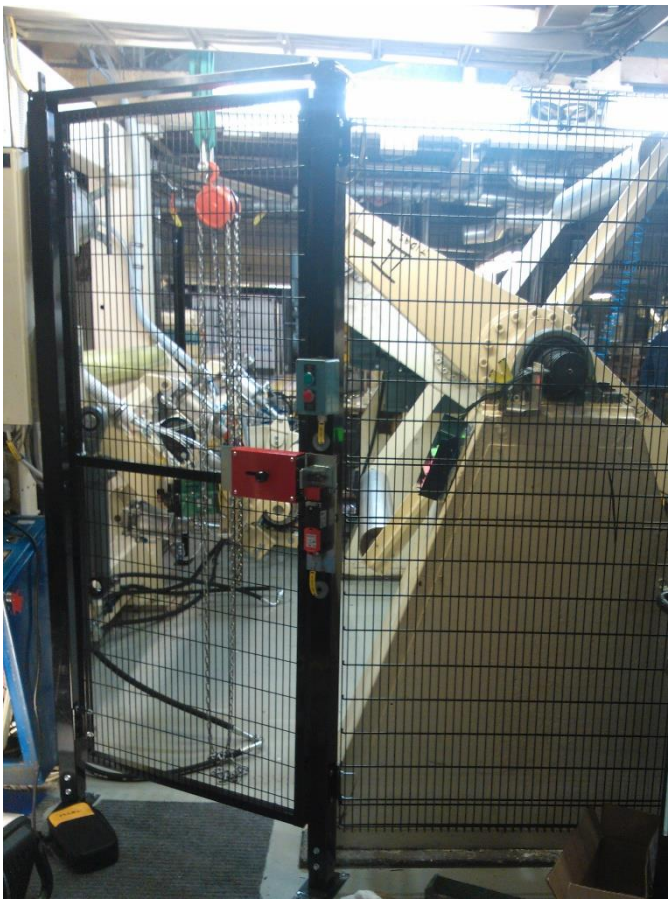
Standardissa SFS 13849-1 edellytetään turvallisuuteen liittyvän ohjausjärjestelmän dokumentointia koko sen elinkaaren ajalta. Tämän vuoksi myös turvatoimintojen testauksesta oli tehtävä dokumentaatio. Esimerkki dokumentista on esitetty liitteessä 10. Testauksessa käydään lävitse mahdollisimman tarkasti koko turva-alue. Testausdokumentissa on eriteltynä kaikki turva-alueeseen kuuluvat turvatoiminnot sekä niihin liittyvät komponentit.

Testaukseen kuuluu periaatteessa kolme osa-aluetta: asennuksien tarkastukset, signaalitestit sekä toiminnallinen testaus. Näistä jokainen käydään siis läpi kunkin komponentin osalta. Asennuksien tarkastuksessa tarkastetaan, että komponentit on asennettu tukevasti niille kuuluville paikoille ja kaapelointi on toteutettu oikein. Tämä tehdään käymällä lävitse jokainen komponentti silmämääräisesti ja mahdollisesti pistokoemaisesti työkalulla kokeillen. Signaalitestissä tarkastellaan turvasignaalien kulkua esimerkiksi oven magneettiselta rajakytkimeltä turvareleelle. Signaalien testaus voidaan toteuttaa silmämääräisesti (esimerkiksi turvareleiden ledien syttyminen) ja mittaamalla jännitteenkoettimella tai muulla sopivalla työkalulla, että signaali tulee perille. Toiminnallisessa testauksessa testataan, että jokainen turvatoiminto toteutuu, kuten on määritelty. Toisin sanoen ovea avataan ja valoverhon läpi kävellään ja tutkitaan, että paineilmat poistuvat, moottorit pysähtyvät jne. Tutkitaan myös, että edellä mainittujen vahinkokäynnistyminen ei ole mahdollista. Pyrkimyksenä toiminnallisessa testauksessa olisi tietysti luoda mahdollisimman monta erilaista skenaariota, joita voi koneella työskennellessä tapahtua. Jokainen tulo ja lähtö tulee testata. Testauksen aikana tulee tarkastella myös turvatoimintojen ja normaalien ohjaustoimintojen rajapintaa sekä näiden vuorovaikutusta toisiinsa. Esimerkiksi jokin koneen normaali ohjaustoiminto ei saa vaikuttaa turvatoiminnon menettämiseen.

Kaikki testauksen vaiheet käydään tarkasti läpi ja huomautukset kirjataan erilliselle kaavakkeelle. Mikäli tulee korjattavaa, tarvittavat korjaukset tehdään ja testi toistetaan. Kun jokainen turvatoiminto on käyty lävitse, voidaan koko turva-alue kelpuuttaa. Testausdokumenttiin tulee kaikkien testauksessa mukana olleiden henkilöiden allekirjoitukset sekä testauspäivämäärä.

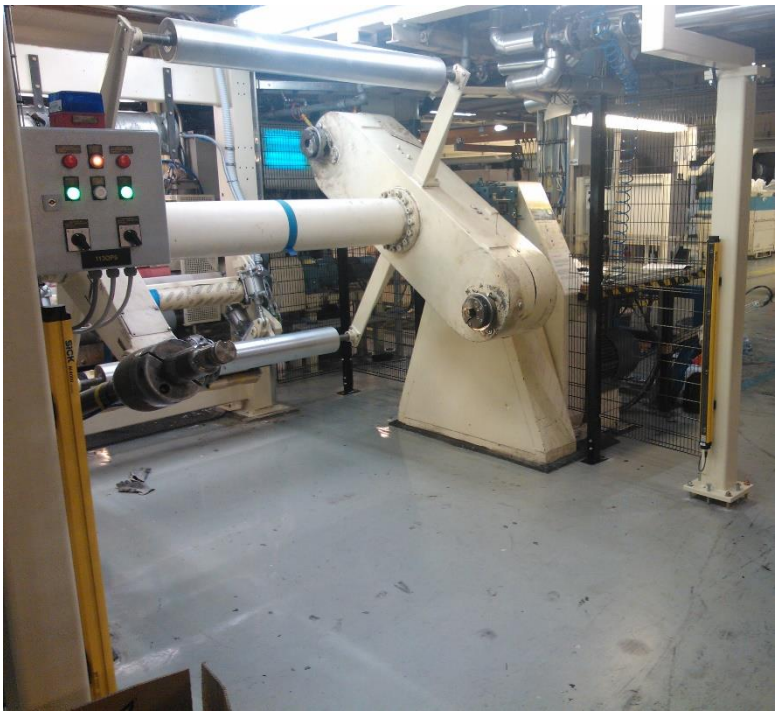
8.2 Valmis turvajärjestelmä

Kiinnirullaimen muutostyöt, joihin turva-alueen lisäys kuului, valmistuivat ajallaan ennen tammikuun loppua. Kuvassa 20 on esitetty valmiin kiinnirullaimen vaihtoalueen uusi turva-aita ja –ovi. Kun verrataan kuvassa 20 näkyvää turva-aitaa kuvassa 13 näkyvään, voidaan todeta uuden suojauksen olevan huomattavasti kattavampi. Kuvassa 20 näkyvät oven salpalukko sekä ovenavaus- ja kuittauspainikkeet. Turva-alueen piirikaaviossa esitetty magneettinen rajakytkin sijaitsee oven ylälaidassa, turva-alueen sisäpuolella. Tällöin turvarajan ohittaminen on hankalampaa. Ovelta on selkeä näkyvyys suojattavalle alueelle, joten oven sulkija näkee onko alueella ketään ennen oven sulkemista ja turva-alueen kuittaamista.



KUVA 20. Kiinnirullaimen turvaovi

Kuvassa 21 näkyy kiinnirullaimen poisottoalue. Kuvaan 14 verrattuna erona on nyt turvaaita, joka estää alueelle pääsyn sivuilta sekä valoverho. Valoverho suojaa edestäpäin pääsemisen karusellille sen ollessa käynnissä. Valoverhon rikkoutuessa karuselli pysähtyy. Kuvan vasemmassa laidassa näkyy uusi ohjauspaneeli, jossa on valoverhoreleen kuittauspainike sekä valintakytkimet. Valintakytkimillä estetään poisottoalueen puolella olevan akselin pyöriminen (kaksi akselia, kaksi kytkintä) sekä sallitaan paineilmojen pääsy paineilmatyökalulle.



KUVA 21. Valoverho kiinnirullaimen poisottoalueella

Turva-alueeseen liittyvät pneumatiikkakotelo, kytkentäkotelo ja hydrauliikka on sijoitettu koneen käyttöpuolelle. Kuvassa 22 on esitetty käyttöjen turvakytkimet sekä kotelot. Kuvan oikeassa ylälaidassa on turva-alueen kytkentäkotelo, joka sisältää mm. Phoenix:n turvareleen. Oikeassa alalaidassa on pneumatiikkakotelo, jossa on radankatkuisulaitetta ohjaavat magneettiventtiilit. Pneumatiikkakotelon yläpuolella on turva-venttiili, jolla kotelon ilmat poistetaan turvatoiminnon kytkeytyessä päälle.

KUVA 22. Turva-alueeseen liittyvät kotelot ja komponentit

8.3 Turva-alueen käyttöönotto

Turva-alueelle tehtiin oma käyttöönottonsa, jossa käytiin läpi yksityiskohtaisesti koko turva-alue. Turva-alueen testauksessa apuna käytin dokumenttia, josta esimerkki liitteessä 10. Testauksessa apunani toimi toinen suunnitteluinsinööri. Aloitimme turva-alueen testaamisen käymällä komponenttien asennukset lävitse silmämääräisesti. Tämän jälkeen siirryimme signaalien testaukseen.

Signaalien testaus aloitettiin testaamalla, että takaisinkytkentätieto tulee jokaiselta piirikaaviossa esitetyltä komponentilta (ks. liite 9). Teimme tämän kytkemällä johtimen irti testattavan komponentin takasinkytkennästä, jolloin pääturvarele lakkasi vetämästä. Turvakontaktorien takaisinkytkennän testasimme pakottamalla kontaktorin mekaanisesti kiinni, jolloin takaisinkytkennän kosketin avautui. Mikäli pääturvareleen valot sammuivat, takaisinkytkentä toimi oikein.

Tämän jälkeen suoritimme toiminnallisen testauksen. Toiminnallisessa testauksessa testasimme ensin, että oven avaaminen aiheuttaa pääturvareleen laukeamisen. Seuraavaksi katsoimme, että turvareleen laukeaminen aiheuttaa muiden turvakomponenttien (turvareleiden ja venttiilien) laukeamisen. Jokainen komponentti oli tarkastettava yksitellen. Testasimme myös valoverhon kävelemällä sen lävitse ja tarkastamalla, että sen ohjaamat turvareleet laukesivat. Karusellin kääntäminen ei ole mahdollista mikäli valoverho on rikkoutunut.

Myös turva-alueen kuittaus testattiin. Mikäli jokin taksinkytkentään kuuluva elementti ei ollut toiminut (kosketin edelleen auki), turvareleen kuittaaminen oven kuittauspainikkeesta ei onnistunut. Kun turvarelettä ei saa kuitattua, mikään sen ohjaama laite ei toimi. Testausvaiheessa huomasimme, että paineilmakotelon turvaventtiili ei toiminut oikein. Kotelon paineilmat eivät poistuneet huolimatta turvarajan rikkoutumisesta. Syyksi paljastui turvaventtiilin pneumatiikkaliitäntöjen väärä kytkentä.

Käyttöönotto turva-alueen osalta sujui hyvin ja ainoaksi virheeksi jäi turvaventtiilin väärä kytkentä, joka saatiin korjattua heti. Turva-alueen voidaan siis todeta toimivan siten, kuin sen on suunniteltu. Testausdokumentti allekirjoitettiin testaajan toimesta ja se arkistoidaan muiden turvallisuuteen liittyvien dokumenttien kanssa.

9 POHDINTA

Työ oli kaikin puolin hyvä esimerkki siitä, miten toteutetaan yksinkertaisimmillaan korkean suoritustason omaava järjestelmä. Vaikka turvallisuuteen liittyvien määräysten ja standardien ymmärtäminen saattaa ensisilmäyksellä tuntua hankalalta, ne ovat loppujen lopuksi yksinkertaisia. Puhtaalla ”maalaisjärjellä” pääsee toimivan turvajärjestelmän suunnittelussa pitkälle. Turvallisuuteen liittyvät standardit eivät ole aina yksiselitteisiä ja niiden tulkinta on aina kiinni siitä, millaista järjestelmää ja millaiseen kohteeseen ollaan toteuttamassa. Kuitenkin käyttämällä yksinkertaisia, hyvin koeteltuja komponentteja, saadaan mielestäni aikaiseksi toimintavarmin järjestelmä. Tämä huomattiin esimerkiksi kiinnirullaimen turvajärjestelmän testausvaiheessa paljastuneiden vikojen vähyydestä.

Toki vaadittavan turvallisuusjärjestelmän vaatimustaso on kiinni myös yrityksen omasta vaatimustasosta. Joskus on helpompi toteuttaa turvajärjestelmä käyttäen turvalogiikoita. Vaikeinta turvallisuuteen liittyvän järjestelmän suunnittelussa on huomioida kaikki siihen kuuluvat osapuolet. Liian monimutkainen turvajärjestelmä lisää vikaantumisen mahdollisuuksia, jotka saattavat johtaa pitkiin ja kalliisiin tuotantokatkoksiin. Turvajärjestelmä ei myöskään saa vaikeuttaa kohteessa työskentelevien työntekijöiden toimintaa. Toisaalta taas yrityksen turvallisuudesta vastaava henkilö/osasto on määrittänyt jonkin tason, joka turvajärjestelmän on täytettävä. Näiden osatekijöiden määrittämissä rajoissa on joskus vaikea lähteä suunnittelemaan itse toteutusta. Yksi kysymys kuuluukin: mihin raja vedetään? Kuinka pitkälle laitteen/kohteen suojaamisessa tarvitsee mennä? Mielestäni tässä työssä esitetyt esimerkkiratkaisut turvajärjestelmälle ovat juuri oikeissa mitoissa. Koneen osa on turvallinen käyttää, täyttää sille vaaditun tason eikä se ole haitaksi koneella työskenteleville.

Minulle työ opetti paljon turvajärjestelmien suunnittelusta sekä niihin liittyvien standardien tulkinnasta ja tutkimuksestani oli toivottavasti hyötyä myös Raflatac Oy:lle. Mikäli tehtaassa turvajärjestelmiä haluttaisiin tutkia lisää tai kehittyä pidemmälle, tulisi tarkastella tarkemmin standardia IEC 62061. Kyseinen standardi käsittelee tarkemmin elektronisi turvajärjestelmiä (turvalogiikat) sekä SIL-luokkia.

LÄHTEET

Apfeld, R., Hauke, M., Rempel, P. & Osterman, B. 2010. The SISTEMA Cookbook 1. From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA. Version 1.0 (EN). Germany: Sankt Augustin.

OEM Finland Oy. 2014. Tuotealue turva. Tulostettu 21.1.2014. http://www.oem.fi/Tuotteet/Turva/531097.html.

Phoenix Contact Oy. 2014. Tuotteet. Releet. Turvatuotteet. Tulostettu 21.1.2014. https://www.phoenixcontact.com/online/portal/fi?1dmy&urile=wcm%3apath%3a/fifi/web/main/products/subcategory_pages/Safety_devices_P-16-03/adda9816-497a-41a9-9b93-0165da519480

Pilz GmbH & Co. KG. 2014. Tuotteet. Tulostettu 23.1.2014. https://www.pilz.com/eshop/b2b/publicinit.do?language=fi&domain=http://www.pilz.com/fi-FI&country=FI&countryIso=FI&isIso=1

SFS-EN ISO 12100. 2010. Koneturvallisuus. Perusteet ja yleiset suunnitteluperiaatteet. 2. painos. Suomen standardisoimisliitto: Helsinki.

SFS-EN ISO 13849-1. 2008. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 2. painos. Suomen standardisoimisliitto: Helsinki.

SICK AG. 2014. Industrial safety systems. Tulostettu 10.2.2014. https://www.mysick.com/saqqara/im0012195.pdf

SITEK-PALVELU OY. 2014. Tuotteet. Asco. Tulostettu 10.2.2014. http://www.sitek.fi/asco

Sundcon Oy. 2014. Turvallisuus. Sistema ohjelmistotyökalu. Tulostettu 20.2.2014. http://www.sundcon.fi/turvallisuus/sistema-ohjelmistotyoekalu